Privacy and Security Toolkit

P A N O R A M A

First Nation Panorama
Deployment in Ontario

Table of Contents

Welcome! 1
Project Background 2
Why Create a Toolkit? 2
What is in this Toolkit? 3
What are the Key Privacy and Security Principles? 4
Privacy Principles from the CSA Model Code 5
Best Practices from the ISO Security Standard 6
What Do I Need to Know about Privacy Laws? 8
    First Nation Laws 8
    Ontario Law – Personal Health Information Protection Act 8
    Federal Law – Privacy Act 9
Getting Started 10
    First Things First 10
    Next Steps 10
Tools List 12
Tool 1 – First Nation Personal Health Information Privacy Assessment 16
Tool 2 – First Nation Personal Health Information Security Assessment 24
Tool 3 – Privacy Policy 33
Tool 4 – Responsibilities of a Privacy Contact 37
Tool 5 – Health Information Privacy and Consent: Frequently Asked Questions - Staff 39
Tool 6 – Confidentiality Agreement 45
Tool 7 – Privacy Notice 47
Tool 8 – Health Information Privacy and Consent: Frequently Asked Questions - Clients 49
Tool 9 – Consent for Using and Disclosing Personal Health Information: A Staff Guide 53
Tool 10 – Consent to Disclose Personal Health Information: General Consent Form & Immunization Data Consent Form 69
Tool 11 – Personal Health Information Inventory 74
Tool 12 – De-Identifying Personal Health Information 78
Tool 13 – Record of Assessment: Determination of Capacity to Provide Consent 81
Tool 14 – Request Form for Personal Health Information Review & Decisions 83
Tool 15 – Security Policy 86
Tool 16 – Business Continuity Management Plan 95
Tool 17 – Access to Network Services Request Form 99
Tool 18 – Acceptable Use Policy 101
Tool 19 – Information Technology Asset Management Inventory 107
Tool 20 – Mobile Devices Security Fact Sheet 110

Table of Contents

First Nation Panorama Deployment in Ontario

Tool 21 – Faxing Personal Health Information Fact Sheet....112
Tool 22 – Privacy and Security Incident Response Plan....116
Tool 23 – Privacy and Security Breach Investigation Report....121
Tool 24 – Notice of Breach - Letter to Client....125
Appendix A – Glossary....127
Appendix B – Health Information Custodian Responsibilities According to PHIPA....134
Appendix C – Additional Resources....135

Copyright © Chiefs of Ontario, 2012. Not to be reprinted or reproduced, in whole or in part, without written permission.

Disclaimer: This document was developed by the Knowledge Management Advisory Group (KMAG), whose partners include the Chiefs of Ontario, Health Canada and the Province of Ontario, for the purpose of the First Nation Panorama Deployment in Ontario. It reflects the priorities, concerns and laws applicable to the partners in Ontario. KMAG partners assume no liability or responsibility for any other use, including use in other jurisdictions.

Funding for this project was provided by the Government of Canada. The opinions expressed in this publication are those of the authors and do not necessarily reflect the official view of Health Canada.

The Authors of this Toolkit

The Knowledge Management Advisory Group (KMAG), through its Privacy and Data Management Working Groups, developed this Toolkit.

Welcome!

If you are reading this Privacy and Security Toolkit, it is likely that you are either preparing to participate in the First Nation Panorama Deployment in Ontario (FNPDiO) Project or considering an eHealth project that involves personal health information. This toolkit was developed for use in the FNPDiO Project and follows accepted Privacy and Security industry standards. However, the information and tools will help you consider important privacy and security issues for any project that involves health information.

Managing personal health information carries important privacy and security responsibilities. Since most people are not privacy and security experts, it can be intimidating to know where to start and how to cover all the key activities. This toolkit is specially designed for First Nations to help identify:

- how to get started:
- essential privacy and security requirements (or "must haves');
- the steps needed to make progress on identified privacy and security gaps, and;
- future privacy and security processes that are recommended (or "nice to have").

Fact

The First Nation Initial Subscribers are:

- Constance Lake
- Couchiching
- Garden River
- Mohawks of Akwesasne
- Nipissing
- Keewaytinook Okimakanak Tribal Council:
  - Deer Lake
  - Fort Severn
  - Keewaywin
  - North Spirit Lake
  - Poplar Hill
- Oneida Nation of the Thames

This toolkit can also help with communicating health information privacy and security information to leaders, community members, and clients.

You don't have to be a privacy and security expert to use this Toolkit or successfully manage your community's privacy and security needs. You also don't need to complete this toolkit by yourself. If you want, assemble a community team to use everyone's expertise and develop broad privacy and security knowledge. The team can include an Elder, your Health Director, a health care professional such as a nurse or physician, Information Technology staff, or another community member who has been asked to lead the privacy and security activities for your First Nation. By using a team, you share both the responsibility and knowledge of privacy and security practices, which will strengthen your overall efforts.

This toolkit will give you a great start in the FNPDiO Project preparing for Panorama, but if you need more information or assistance, you can contact the FNPDiO Project personnel identified in the team directory accompanying this Toolkit.

Project Background

Fact

Health information may be personal to one individual or it may be grouped together (or "aggregated") to show the big picture for a community, zone or region. Health information about a single identifiable person is called Personal Health Information or PHI.

Important

Authorized Users: All Panorama users must be authorized by their organizations to get access to Panorama. Authorized users will only access the Panorama system for health purposes.

This tripartite project began in 2006 when the Chiefs of Ontario (COO) completed an environmental scan to support the development of a First Nations approach to public health in Ontario. The scan identified four key priority areas: pandemic preparedness, jurisdictional clarity, resourcing, and surveillance.

Based on these recommendations, First Nation leadership passed Resolution 06/47 at the 32nd All Ontario Chiefs Conference. A key result was the creation of the Knowledge Management Advisory Group (KMAG) to provide strategic guidance for an integrated public health information management system for First Nations.

The FNPDiO Project is a First Nation-led tripartite initiative, guided by eleven First Nation Initial Subscribers. First Nations in Ontario became involved to ensure that Panorama is responsive to our unique public health needs. The three partners in this project include the Chiefs of Ontario, the First Nations and Inuit Health Branch – Ontario Region of Health Canada, and the Ontario Ministry of Health and Long-Term Care.

Disclaimer

References to Personal Health Information (PHI) and *Personal Health Information Protection Act* (PHIPA) requirements apply specifically to Health Information Custodians (HIC's) under PHIPA, including First Nation health facilities. These references and requirements do not apply to health facilities operated by Health Canada, which are governed by the federal Privacy Act..

Why Create a Toolkit?

This Toolkit was developed for several reasons – the first of which was to support Panorama deployment among First Nations. First Nations, through the provision of health services (such as immunization) have specific responsibilities as keepers of personal health information. It was also recognized that First Nations might not have formal privacy and security materials in place or may not have the necessary resources to develop such materials. It was agreed that a tool to support communities with the most important privacy and security issues was needed, and that any materials developed should help communities put these pieces in place quickly and effectively. Having all the essential materials available in a single toolkit reduces the burden on communities and speeds the process of getting ready to participate in a health related project.

Finally, it was recommended that communities should be able to use this toolkit for more than just Panorama. It should be useful for all types of eHealth or health related privacy and security activities.

What is in this Toolkit?

This version of the toolkit is intended to be a first draft or 'work in progress' for testing purposes. As the various tools are used by Initial Subscribers, we anticipate changes from the FNPDiO pilot and Lessons Learned documents that will be part of the early phases of deployment. Although this document will continue to evolve and change in response to the needs of First Nations, it was important not to delay it until everything was perfected or every possible use was known. Important lessons will come from the use of the tools and will guide future content.

Important

There are many benefits for clients and health care professionals because of increased access to PHI through Panorama and other eHealth initiatives. Keeping information private and secure must remain a top priority.

This first version of the toolkit contains several tools that can be used to prepare for the privacy and security requirements of participating in Panorama or other eHealth projects. These tools can be used to create policies and procedures or improve existing ones.

The Toolkit includes:

- Questionnaires for assessing current privacy and security practices
- Forms to collect information or record consent
- Guides for disclosing information or identifying practices supporting privacy
- Sample Policies
- Tips
- Frequently Asked Questions (FAQs)
- Glossary of terms used in this toolkit
- Additional resources that can be used at a later date.

What are the Key Privacy and Security Standards?

Fact

The Canadian Standards Association's (CSA) Model Code for the Protection of Personal Information balances the privacy rights of individuals with the information requirements of organizations that use the information.

There are many privacy and security standards, some international and some specific to Canada. This toolkit was developed using the most current and widely used privacy and security standards in Canada.

The two most important standards are presented here so you will be familiar with them. You don't need to memorize them, but it's helpful to be aware of them and understand their overall guidance. The first is a Canadian privacy standard, and the second is the most important international standard that guides security activities in Canada.

The two standards are identified below and are presented on the next page for your information:

- Canadian Standards Association (CSA) Model Code for the Protection of Personal Health Information.
- ISO 27002 Information technology - Security techniques - Code of practice for information security management.

Privacy Principles from the Canadian Standards Association (CSA) Model Code

There are ten commonly accepted principles found in the CSA Code that guide the protection of PHI. You will recognize them as they appear in many tools in this Toolkit.

Principles for the Protection of Personal Information	
1	Accountability Each health facility that collects PHI must put someone in charge of making sure privacy policies and practices are followed.
2	**Identifying Purposes** Clients must be told why their personal information is being collected when or before it is collected.
3	**Consent** Clients must agree (or "consent") to the collection, use and disclosure of their personal information.
4	**Limiting Collection** Only information that is required should be collected.
5	**Limiting Use, Disclosure And Retention** PHI can only be used or disclosed for the purpose that it was collected. Added consent is required for any other purposes. Personal information should only be kept as long as necessary.
6	**Accuracy** Every effort to reduce the risk that incorrect PHI is used or disclosed.
7	**Safeguards** Health facilities must protect PHI from loss or theft. They must create safeguards to prevent unauthorized access, disclosure, copying, use or modification.
8	**Openness** Health facilities must make their privacy policies easily available to clients.

9	**Individual Access** Clients have the right to ask to see their personal information. They have the right to know who has access to their PHI and to whom their PHI may be disclosed. They can question the accuracy of their personal information and ask for corrections.
10	**Challenging Compliance** Clients must be able to challenge a health facility's privacy practices.

Best Practices from the ISO Security Standard (ISO 27002)

The key document for almost all security standards in Canada is ISO 27002. It was developed by the International Organization for Standardization (ISO). ISO recommends "best practices" for the protection of confidentiality, integrity, and availability of information by focusing on eleven key areas. Many tools in this Toolkit are the result of this standard.

Best Practices for the Protection of Personal Information within your First Nation health facility	
1	**Security Policy** Develop a written information security policy.
2	Organization of Information Security Assign responsibility for security and control use of information by third parties.
3	**Asset Management** Identify someone to be responsible for information technology equipment (or "assets"), such as computers and smart phones, and use a system to classify and track these assets.
4	**Human Resources Security** Focus on security before, during, and at the end of employment for all staff, contractors, students, and volunteers. Make sure that individuals know about their responsibilities for PHI security.
5	**Physical and Environmental Security** Protect the part of your facility that contains information technology. Protect equipment from risk of loss or damage.

Best Practices for the Protection of Personal Information within your First Nation health facility	
6	**Communications and Operations Management** Develop and use operational procedures that ensure system security.
7	**Access Control** Control who can get access to information, networks, applications and operating systems.
8	**Information Systems Acquisition, Development and Maintenance** Build security into information technology systems and software, and regular system maintenance.
9	**Information Security Incident Management** Identify security requirements and use appropriate security tools and procedures for managing incidents.
10	**Business Continuity Management** Use business continuity management to protect information in the event of disasters or other hazards.
11	**Compliance** Identify legal and policy requirements and perform regular reviews to make sure the rules are being followed.

What Do I Need to Know about Privacy Laws?

First Nation Laws

Each First Nation in Ontario has jurisdiction to create their own laws, including privacy laws. A First Nation that had passed its own privacy law would have to review the law to see how it applies to Panorama or other eHealth projects.

If your community does not have a First Nation law relevant to privacy or health information, Ontario's Personal Health Information Protection Act (PHIPA) applies to guide appropriate health information collection, use and disclosure. Most health facilities will use PHIPA as their key guide for information privacy.

Ontario Law – Personal Health Information Protection Act

Fact

PHIPA protects the privacy of personal health information of every person in Ontario. A First Nation operating a health facility (First Nation health facility) is considered to be a "Health Information Custodian" in PHIPA.

The Personal Health Information Protection Act (PHIPA) is an Ontario provincial law. It applies to health facilities, including those operated by First Nations, if there is no applicable First Nation law.

PHIPA sets the rules for the collection, use, and disclosure of PHI by Health Information Custodians (HICs). PHIPA also:

- Makes First Nation health facilities responsible for "agents" - such as regular staff, and contract staff, students, volunteers, or service providers - who collect, use or disclose PHI on their behalf.
- Requires naming a Privacy Contact person
- Requires HICs to have a public written statement that explains how PHI is collected, used and disclosed.
- Requires that HICs keep accurate records of PHI. It creates rules for clients to access their PHI and request a correction if they believe there is an error.
- Describes the circumstances in which health information can be disclosed both within and outside of the health facility.
- Provides rules for client consent and the use of substitute decision-makers
- Promotes sharing PHI in appropriate ways so that clients can receive and benefit from integrated health services.
- Identifies the responsibility of the Information and Privacy Commissioner of Ontario to make sure organizations follow PHIPA requirements and directions.

Fact

PHIPA focuses on outcomes without being specific about how to accomplish them. This Toolkit provides best practice on how to achieve the outcomes and meet requirements.

Appendix B contains more information on the responsibilities of HICs. You can use this information in your role as a leader or representative of your health facility, but you may want to share this type of information with your Band Council or other community leaders so everyone understands the responsibilities of the HIC.

Federal Law – Privacy Act

The *Privacy Act* is a federal law that regulates how federal institutions deal with personal information. The Privacy Act applies only to those health facilities that are operated by Health Canada in First Nation communities. The Health Canada staff working in those facilities must follow the Privacy Act.

Fact

The Privacy Act applies only to Health Canada-operated health organizations, not to First Nation-operated health organizations.

The *Privacy Act* requires that staff must:

- Only collect personal information related directly to a federal program or service;
- If possible, inform clients about the purpose for which personal information is collected;
- Use personal information only for the purpose it was collected. Most of the time the individual needs to give their consent for any other use; and
- Not disclose personal information under their control, unless the client gives consent.

Getting Started

First Things First

There are three key steps:

1. Assess
2. Address
3. Review

However, before you begin, the first activity is to identify a Privacy Contact. This person will be responsible for privacy in your Organization. Depending on your Organization, the Privacy Contact may or may not also be the person responsible for Security. Depending on the size of your community, the Privacy Contact may be a Health Director, Community Health Nurse, or another trusted individual with responsibility for health care.

Some communities may also decide to set up a Privacy Committee or Working Group that can assist in reviewing and revising policies and procedures when required.

Next Steps

Important

Three steps to privacy & security:

Assess, Address & Review.

The Privacy Contact will lead the use of the Toolkit, beginning with the Privacy Assessment and the Security Assessment. As mentioned, the information and tools contained in this Toolkit meet the privacy and security requirements for First Nations implementing Panorama. However, health facilities may also use this Toolkit for other projects with privacy and security needs.

This toolkit was designed to assist in addressing all of the key privacy and security policies and procedures - or those "must have" parts. In some cases, additional recommended ("nice to have") tools are also provided. Each tool is described below and is clearly marked whether it is required ("must have"), strongly recommended, or optional ("nice to have").

Tools 3-24 in this toolkit can all be adapted to meet the unique needs of your First Nation. As a result of existing community activities, such as Emergency Preparedness Planning, you may already have some tools (or parts of tools) in place. If this is the case, you may wish to use this toolkit to identify gaps and update your policies.

1	**ASSESS…** This first step assesses the current state of privacy and security controls related to collecting, using and disclosing personal information and PHI in your health facility (Tools 1 and 2). Once completed, you will have identified any gaps or areas you need to address. (Gaps or areas needing attention will be any questions answered as 'No' or 'Partial".)
2	**ADDRESS…** The second step is to address the gaps identified in the ASSESS PHASE by using the tools provided in the Toolkit (Tools 3 – 24). You can use all the tools in two ways. You can adopt the tools "as is" and simply place your community name and logo (if available) on the document before you start to use it. This will make it clear that your health facility has reviewed the document and adopted it. The second way to use the tools is to revise them. All tools in this document can be revised or changed to meet your community's needs. Each First Nation may have its own internal processes for adopting or revising policies and procedures. One process may be for the Health Department to review the relevant documents and make recommendations to Chief and Council or Health Board on adopting the policies and procedures.
3	**REVIEW…** The third step is to review your new policies and procedures developed in the ADDRESS phase against the assessment tools used in the ASSESS phase to make sure that all the gaps have been addressed.

Tools List

Below is a summary and a short description of all the tools in this Toolkit. Beside each description is a letter that tells you if the tool is Required, Strongly Recommended or Optional. The tools are organized to be available as you go through the assessments. For example, as you answer questions in the Privacy Assessment (Tool 1), you may find that you have a gap or need a tool. The tools that you may need first will be located at the beginning, while tools that you might need as you complete the Security Assessment (Tool 2) will be located in the later parts of the toolkit.

Legend: **R = Required ("Must Have" due to legal obligations under PHIPA)** **S = Strongly Recommended** **O = Optional ("Nice to Have")**

STEP 1 ASSESS Tools Summary	
Tool #1: First Nation Personal Health Information Privacy Assessment	
R	This tool is used to identify any gaps in the current state of privacy policies and procedures in any First Nation health facility. It will assist you in identifying privacy issues for both Panorama-specific and general electronic health information needs.
Tool #2: First Nation Personal Health Information Security Assessment	
R	This tool is used to identify any gaps in the current state of security policies and procedures in any First Nation health facility. It will assist you in identifying security issues for Panorama-specific needs as well as general electronic health information needs.
STEP 2 ADDRESS Tools related to Information Privacy	
Tool #3: Privacy Policy	
R	A Privacy Policy defines how your Organization protects clients' personal privacy under PHIPA. This is a required document and guides the actions of your employees, contractors, and volunteers. A sample Privacy Policy is provided.
Tool #4: Responsibilities of a Privacy Contact	

S	This document is a role description for the Privacy Contact. PHIPA requires someone in your Organization to be designated as the Privacy Contact. This tool describes their legal responsibilities under the Act. Although not required, it is strongly recommended to have this information either as a separate description for the Privacy Contact or included as part of another role description (or job description).
Tool #5: Health Information Privacy and Consent: Frequently Asked Questions - Staff	
O	This FAQ addresses some of the most frequently asked questions about privacy.
Tool #6: Confidentiality Agreement	
R	Confidentiality Agreements must be signed by everyone (e.g. health staff, data entry clerks or information technology staff) who has access to PHI. This is a required document that protects clients' information, your Organization, and commits the signing person to follow the policies and procedures of the Organization.
Tool #7: Privacy Notice	
R	PHIPA requires that HICs have a written statement for clients to tell them about the collection, use and disclosure of PHI. The Privacy Notice meets this requirement.
Tool #8: Health Information Privacy and Consent: Frequently Asked Questions - Clients	
O	This is a set of frequently asked questions about privacy and is written for your clients.
Tool #9: Consent for Using and Disclosing Personal Health Information: A Staff Guide	
S	This tool is a guide to help staff manage consent in a consistent way. It includes descriptions of different situations to help staff understand the kinds of consent required, e.g. implied consent, express consent, no consent.
Tool #10: Consent to Disclose Personal Health Information: General Consent Form and Immunization Data Consent Form	
S	Immunization records are considered PHI under law. In some situations a 'Consent to Disclose Immunization Information' form must be completed and signed before a health facility can disclose immunization record information to a third party. In other situations, a general form may be sufficient. These forms can be used as is, or adapted to your community needs.
Tool #11: Personal Health Information Inventory	
S	This tool allows HICs to manage and know exactly what PHI is kept, where it is, and who is responsible for it. This inventory can be very important if an incident such as a computer failure or lost memory stick occurs.
Tool #12: De-identifying Personal Health Information	

S	PHIPA requires HICs to collect, use, and disclose the minimum amount of PHI necessary for the purpose. This tool describes how to remove information from a record that could identify a client when sharing or combining health information. Although this tool is not required, there will be times when information should be made anonymous for sharing or reporting purposes.
Tool #13: Record of Assessment: Determination of Capacity to Provide Consent	
S	Staff may be required to determine if a client is unable to give consent for their care and PHI. If not already documented in the client's chart or another format (e.g. progress notes), this form can be used to document the assessment of the capacity of a client to give informed consent for the collection, use or disclosure of their PHI.
Tool #14: Request Form for Personal Health Information Review & Decisions	
O	PHIPA gives clients the right of access to PHI by making a written request. Clients may request a correction if they believe their record is inaccurate or incomplete. This tool creates a log of written client requests to access their PHI and any resulting decisions or actions taken by the Organization as a result of the client request.
STEP 2 ADDRESS Tools related to Information Security	
Tool #15: Security Policy	
R	A Security Policy is a standard requirement in any organization that handles personal information. Security policies describe the requirements staff members are expected to follow to support the security of personal information.
Tool #16: Business Continuity Management Plan	
S	A Business Continuity Plan (BCP) identifies what you need to do to protect client information in the event of an emergency. You may already have this included in your Emergency Preparedness Plan and if not, this tool may assist you.
Tool #17: Access to Network Services Request Form	
S	This form can be used to manage the process of responding to requests by staff, contactors, and volunteers for access to the computer network and systems.
Tool #18: Acceptable Use Policy	
S	An Acceptable Use Policy guides staff as they access the computer network and systems, including the Internet.
Tool #19: Information Technology Asset Management Inventory	
O	This tool is a form to record information about servers, monitors, keyboards, laptops, mobile devices, phones, software and licenses, etc to assist with the management of an information technology system.

Tool #20: Mobile Devices Security Fact Sheet	
O	This is a guide for all employees, contractors, and volunteers and covers the privacy aspects of smart phones, laptops, tablets and USB keys, including a "10 Privacy Tips" list.
Tool #21: Faxing Personal Health Information Fact Sheet	
S	A list of best practices in communicating PHI by fax.
Tool #22: Privacy and Security Incident Response Plan	
S	This tool describes how to recognize privacy and security incidents / breaches. It outlines a four-step process to identify and respond to incidents, and includes a suggested process that can be adapted for community use.
Tool #23: Privacy and Security Breach Investigation Report	
S	A form that can be used to record the details of an incident to assist in preventing future incidents.
Tool #24: Notice of Breach – Letter to Client	
R	This tool is a notice for contacting individuals if their information has been (or is at risk of being) inappropriately accessed or disclosed. Contacting clients whose information is involved in a breach is required by PHIPA.
STEP 3 REVIEW Tools	
Now that you have completed the review of tools and development of any required materials, you can go back to Tools 1 and 2 from STEP 1 to confirm the gaps have been addressed.	

This Toolkit also contains the following appendices as additional resources to support use of the Toolkit.

Appendix A - Glossary

A set of definitions for key words used in this Toolkit

Appendix B - Health Information Custodian Responsibilities According to PHIPA

A guide to help understand the role and responsibilities of the HICs under PHIPA.

Appendix C - Additional Resources

A list of additional information and resources that may be helpful.

Tool #1
First Nation Personal Health Information Privacy Assessment

Instructions

This tool will help you review information privacy controls for Personal Health Information (PHI) at your First Nation health facility. Privacy controls can be policies, procedures, agreements, notices, or other measures applied within your Organization. This tool will also identify any issues or gaps in your privacy controls.

The questions are based on the ten principles of the CSA's Model Code for the Protection of Personal Information described in the Introduction section of this Toolkit.

Completing the Assessment Tool

Answer each question with Yes, No, Partial, or Not Applicable as described below. To answer "Yes", the control must be written and in use by staff, contractors, students and volunteers. You don't always need separate documents for each privacy control as long as the content is written and available. One exception is the Privacy Notice that must be developed and publically posted.

A "No" or "Partial" answer to any question indicates a potential privacy gap. The right column in this assessment has links to other toolkit resources to help you correct identified gaps with the most relevant and important resources listed first. Even if you answer "Yes" or "N/A", it may be helpful to check the tools to make sure that your current privacy controls are complete.

Yes	Yes, the privacy control is written, is complete, and is used consistently.
No	No, there is no written privacy control.
Partial	The privacy control is written but is not complete or not always used.
N/A	Not applicable. This question does not apply to this First Nation health facility.

Be aware…

Once completed, the Privacy Assessment will contain sensitive details about your information privacy. It is important to protect this information.

INSERT YOUR LOGO HERE

First Nation Personal Health Information Privacy Assessment

General Information	
First Nation Health Facility:	
Date:	
Contact Information - Person Responsible for the Assessment	
Name:	
Email:	
Phone:	
Role/Position:	

Roles and Number of Staff

This section only needs to be completed once – either in Tool 1 or Tool 2.

This is a summary of the roles and users in your health facility that may have access to Personal Health Information (PHI). All persons with access to PHI should receive training and sign confidentiality agreements. You can use this summary to identify the appropriate type of training and confidentiality agreement.

The Role column describes the types of services performed in your facility. The three columns to the right show the different types of employment roles individuals may have with your facility:

- *"Staff" are paid employees;*
- *"Contractors" are people who are paid to provide services to your facility but are not employees. They may have a service contract that defines their scope of work and requirements for confidentiality;*

"Volunteers" are not paid by your health facility but may still have access to PHI. Volunteers can include health care students or others.

Role	# of Staff	# of Contractors	# of Volunteers
Receptionist			
Clerk			
Community Health Representative			
Nurse/Nurse Practitioner			
Physician			
Health Director			

Information Technology			
Janitorial			
Students			
Others (please specify as applicable)			

Privacy Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Reference
Organization and Accountability for Information Privacy: Effective information privacy depends on both law and best practices. Legally, First Nation health facilities are considered "Health Information Custodians" or HICs. HICs have the responsibility to ensure the privacy of PHI that they collect, use, and disclose.					
1. Does the health facility have a written privacy policy to protect PHI in their custody or control?	☐	☐			3
2. Has an individual been assigned to be responsible for Information Privacy (the "Privacy Contact")?	☐	☐			3 (For additional reference: 4, Appendix B)
3. Does the Privacy Contact have a written role description and responsibilities consistent with PHIPA? If yes, does it:	☐	☐			4
a. Support the HIC's compliance with PHIPA	☐	☐			3, 4 (For additional reference: Appendix B)

Privacy Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Reference
b. Ensure all staff, contractors, students and volunteers are informed about their duties under PHIPA	☐	☐			3, 4 (For additional reference: Appendix B)
c. Ensure all staff, contractors students and volunteers with access to PHI have signed confidentiality agreements	☐	☐			3, 4 (For additional reference: Appendix B)
d. Respond to inquiries about the HIC's information practices	☐	☐			3, 4 (For additional reference: Appendix B)
e. Respond to requests for access to or correction of PHI	☐	☐			3, 4 (For additional reference: Appendix B)
f. Receive complaints about possible failure of the HIC to meet the requirements of PHIPA	☐	☐			3, 4 (For additional reference: Appendix B)
4. Has the Privacy Contact received training on his or her responsibilities?	☐	☐			FNPDiO Training Materials
5. Are specific individual(s) assigned tasks that support the health facility in meeting its HIC responsibilities? (eg., delivering privacy training, developing and approving policies, incident management, etc.)	☐	☐			Appendix B
6. Are there policies to manage the sharing of PHI outside of the health facility?	☐	☐			3

Privacy Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Reference
Collection, Use, Disclosure and Disposal: PHIPA identifies the responsibilities of HICs to limit the collection, use, and disclosure of PHI to only what is necessary for the stated purpose, and to manage PHI in ways that are consistent with the client's informed consent. The Security Assessment (Tool #2) covers procedures for authorizing access to PHI.					
7. Is there a written policy that PHI is only collected, used, or disclosed for the purposes consistent with the client's consent, Privacy Notice, or otherwise as permitted by law?	☐	☐			3 (For additional reference: 7, 8, 9,10, Appendix B)
8. Is there a written policy on recording the types of PHI collected and where it is stored?	☐	☐			3 (For additional reference: 11)
9. Are practices in place to de-identify PHI so that client privacy is protected?	☐	☐			12
10. Is PHI made anonymous when used for planning, forecasting, reporting, and/or evaluation purposes?	☐	☐			12
11. Is there a schedule for how long to keep PHI and how to safely dispose of it?	☐	☐			3
Consent: PHIPA has a strong focus on the protection of clients and consent. The HIC must obtain clients' consent to collect, use, or disclose PHI.					
12. Is there a written policy regarding consent? If yes, does it include:	☐	☐			3 (For additional reference: 7, 8, 9, 10)
a. When consent is collected?	☐	☐			3 (For additional reference: 7, 8, 9, 10)

Privacy Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Reference
b. That consent is obtained directly from the client. If not, why?	☐	☐			3 (For additional reference: 7, 9, 10)
c. Procedures to ensure that the client has the capacity to give consent?	☐	☐			3, 13
d. Procedures to identify individuals who are approved to make decisions on behalf of others (e.g. custodial parents, customary care arrangements)	☐	☐			9, 13
Accuracy: HICs have a responsibility to ensure that PHI is as accurate, complete and up-to-date as needed for its purpose.					
13. Is there a written policy to ensure that PHI is accurate, complete and up-to-date? If yes, do the requirements include the following for all updates:	☐	☐			3
a. Time and date	☐	☐			3
b. Who updated the record	☐	☐			3
c. Source of updates and changes (e.g., parent, guardian, etc.)	☐	☐			3
Safeguards: HICs must protect PHI from loss or theft. Safeguards to prevent unauthorized access, disclosure, copying, use, or modification must also be in place.					
14. Is there a written policy regarding privacy training requirements?	☐	☐			3, 4

Privacy Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Reference
15. Is there a written policy requiring all staff, contractors, students and volunteers to sign a confidentiality agreement?	☐	☐			3, 6
16. Are activities monitored or audited to confirm that individuals only look at PHI they need to perform their job?	☐	☐			3, 15, 18
Open-ness: HICs must have a written privacy statement. This is done most often by posting a Privacy Notice in a public area of your facility.					
17. Is a written Privacy Notice available to community members? If yes, does it contain the following:	☐	☐			3, 7
a. Why the facility collects PHI.	☐	☐			7
b. How to reach the Privacy Contact.	☐	☐			7
c. How a client can access his/her records.	☐	☐			7
d. How a client can request a correction to his/her record.	☐	☐			7
e. How to make a privacy complaint regarding the handling of PHI.	☐	☐			7
f. How to contact the Information and Privacy Commissioner of Ontario.	☐	☐			7
Client Rights: Clients have a number of rights about their PHI. These include the right to ask to see any of their PHI, and request corrections if they feel the information is incomplete or has errors, and the right to challenge the First Nation health facility's privacy practices.					
18. Is there a written policy for individuals to:					

Privacy Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Reference
19. Request access to their PHI	☐	☐			3 (For additional reference: 7, 14)
20. Request a correction to their PHI.	☐	☐			3 (For additional reference: 7, 14)
21. Is there a procedure to ensure that individuals are notified that a correction to his/her information has been made?	☐	☐			14
22. Does the facility have a complaint procedure about their privacy practices?	☐	☐			3 (For additional reference: 7)
23. Is a record kept of the following:					
24. Requests for a review of errors or omissions.	☐	☐			14
25. Decisions about corrections (e.g., amendments or decisions not to amend).	☐	☐			14

Tool #2
First Nation Personal Health Information Security Assessment

Instructions

This tool will assist you to review information security controls for Personal Health Information (PHI) in your health facility and identify any issues or gaps that may need to be addressed. Security controls can be policies, procedures, agreements, notices, or other measures.

Completing the Assessment Tool

Answer each question with "Yes", "No", "Partial", or "Not Applicable" as described below. To answer "Yes", the control must be written and in use by staff, contractors, students and volunteers. Separate documents are not needed for each security control as long as the content is written and available.

A "No" or "Partial" answer to any question indicates a potential security gap. The right column in this assessment has references to other toolkit resources to help you correct identified gaps. If you answer "Yes" or "N/A", it may be helpful to check the tools to make sure that your current security controls are complete.

Yes	**Yes**, the security control is written, is complete, and is used consisently.
No	**No**, there is no written security control.
Partial	The security control is written but is not complete or not always used.
N/A	**Not applicable**. This question does not apply to this First Nation health facility.

Be aware…

Once completed, this Security Assessment will contain sensitive details about the protection and security your health facility's information. It is important to protect this information.

INSERT YOUR LOGO HERE

First Nation Personal Health Information Security Assessment

General Information	
First Nation Health Facility:	
Date:	
Contact Information - Person Responsible for the Assessment	
Name:	
Email:	
Phone:	
Role/Position:	

Roles and Number of Staff

This section only needs to be completed once – either in Tool 1 or Tool 2.

This information creates a summary of the roles in your health facility that may have access to Personal Health Information (PHI). All persons with access to PHI should receive training and sign confidentiality agreements. You can use this summary to identify the appropriate type of training and confidentiality agreement.

The Role column describes the types of services performed in your facility. The three columns to the right show the different types of employment roles individuals may have with your facility:

- *"Staff" are paid employees;*
- *"Contractors" are people who are paid to provide services in your facility but are not employees. They may have a service contract that defines their scope of work and requirements for confidentiality;*

"Volunteers" are not paid by your health facility but may still have access to PHI. Volunteers can include health care students or community members.

Role	# of Staff	# of Contractors	# of Volunteers
Receptionist			
Clerk			
Community Health Representative			
Nurse/Nurse Practitioner			
Physician			
Health Director			
Information Technology			
Janitorial			
Students			

Roles and Number of Staff			
Others (please specify as applicable)			

Security Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Ref
Organization and Accountability for Security: It is best practice for the First Nation health facility to have a written security policy and to identify who has responsibility for information security.					
1. Is there a written security policy to protect PHI in the facility's custody or control?	☐	☐			15
2. Has an individual been assigned the responsibility for Information Security?	☐	☐			15
3. Is authorization responsibility assigned to prevent conflict of interest? (e.g. the person requesting access to PHI is not the same person approving access)	☐	☐			15
Physical and Environmental Security: It is best practice to protect equipment from risk of loss or damage, as well as the facilities that contain information technology and systems. Many facilities include this in their disaster plans.					

Security Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Ref
4. Is the physical security of information assets protected from loss, vandalism, or environmental hazards such as fire and flood?	☐	☐			15 (For additional reference: 16, 20)
5. Do the facility's computers and other system devices have battery back up to cover power failure?	☐	☐			15 (For additional reference: 16)
6. Are there procedures to protect PHI from public view?	☐	☐			15
7. Are there procedures to manage access to secure areas of the facility (e.g. key management, sign in, and auditing)?	☐	☐			15
Access to PHI and Information Systems: Many security best practices help control access to information, networks, applications, and operating systems. These should be in place before granting access to systems or information.					
8. Are access controls in place to protect the following systems? (Example controls could include firewalls, user passwords, and role-based access)					
a. Controls for access to a local area network (including wireless access) from within the facility.	☐	☐			15 (For additional reference: 17)
b. Controls for access to administrator or system management functions and applications.	☐	☐			15 (For additional reference: 17)
c. Controls for access to clinical applications or databases.	☐	☐			15 (For additional reference: 17)
d. Controls for remote on-line access (e.g. accessing clinical applications from home).	☐	☐			15

Security Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Ref
9. Are there written procedures for authorizing staff access to PHI? If yes, does it include the following:	☐	☐			15 (For additional reference: 17, 18)
a. A definition of who needs to approve access.	☐	☐			15 (For additional reference: 17)
b. Roles and job duties within the facility (e.g. clerks need access to less information than nurses or physicians).	☐	☐			15 (For additional reference: 3)
c. A unique user name for each authorized user so there is no sharing of accounts.	☐	☐			15
d. A requirement for users to follow rules for creating strong passwords to access PHI? (e.g. containing upper case, lower case, numeric and symbols).	☐	☐			15
e. A written process to quickly disable user accounts? (e.g. within 24 hours).	☐	☐			15 (For additional reference: 17)
Human Resources Security: People's actions are important to maintaining the information security. First Nation health facilities should emphasize security prior to, during, and at the end point of work or volunteer roles.					
10. Is there a written policy to ensure:					-
a. Security responsibilities are included in the terms and conditions of employment, service contracts, or volunteer activity.	☐	☐			5 (For additional reference: 6)
b. Background reference checks are conducted before hiring new staff or accepting new volunteers.	☐	☐			15

Security Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Ref
11. Is there a written policy to guide acceptable use of network access and systems?	☐	☐			18
Managing your Systems: It is best practice to have a current list of all computer systems and equipment. Monitoring security processes is part of the day-to-day management of your information systems.					
12. Is there a written procedure to manage information assets (e.g. assignment of responsibilities, inventory, and procedures for secure disposal/re-use)?	☐	☐			15 (For additional reference: 19)
13. Is there a written policy for technology maintenance (such as patches, emergency fixes or system updates)?	☐	☐			15
14. Is there a written policy to maintain protection against Malicious and Mobile Code (e.g. computer viruses, worms, etc.)?	☐	☐			15
15. Are regular Backup / Restore processes for information systems and data used?	☐	☐			15 (For additional reference: 16)
16. Are information systems monitored for security risks? (e.g. review of firewall logs)	☐	☐			15
17. Are policies in place guiding when general security audits should be done?	☐	☐			15
18. Are records of network or system access kept for audit purposes? If so:	☐	☐			15
a. Is access recorded, capturing the user's login name, date and time of access, system/application accessed, and action taken (read, write, delete)?	☐	☐			15

Security Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Ref
b. Are the records of access to PHI kept for a specified period of time and protected from tampering?	☐	☐			15
Communications and Operations Management: It is best practice to develop and implement procedures that uphold system security. These written procedures guide staff to consistently carry out security practices in their daily work.					
19. Is there a written policy covering the use of mobile devices such as laptops and smart phones, and portable storage media (e.g. portable hard drives, memory cards, USB flash drives, CDs or DVDs containing PHI)?	☐	☐			15 (For additional reference: 20)
20. Is there a written control to ensure that any removal of information assets from the facility is authorized (e.g. files, computers, etc)?	☐	☐			15 (For additional reference: 20)
21. Is there a written policy or procedure to guide access to PHI from outside the facility (e.g. from home)?	☐	☐			15 (For additional reference: 20)
22. Is there a written policy or procedure that desks and computer monitors must be kept clear of PHI when unattended (i.e. Clear Desk / Clear Screen)?	☐	☐			15
23. Do work stations time out after periods of inactivity?	☐	☐			15
24. Is there a written policy for the secure transfer of PHI (e.g. use of encrypted email, faxes)?	☐	☐			15 (For additional reference: 21)

Security Assessment					
Questions	Answers				
	Yes	No	Partial (Explain)	Not Applicable (Explain)	Toolkit Ref
Incident Management: Best practice requires a First Nation health facility to manage PHI security incidents using appropriate security tools and procedures.					
25. Is there a written procedure for Incident Management for:					15 (For reference: 22, 23, 24)
a. Detection of privacy or security breaches	☐	☐			
b. Escalation Process	☐	☐			
c. Containment	☐	☐			
d. Investigation	☐	☐			
e. Reporting	☐	☐			
f. Notification of any affected individuals	☐	☐			
g. Lessons Learned Documentation	☐	☐			

Step 2: ADDRESS

Once privacy and security readiness has been assessed for Panorama, the tools in this section address any gaps identified. Tools follow the order of questions in the Privacy and Security Assessments.

- **Tools 3-14** focus on information privacy/
- **Tools 15-24** focus on information security. In some cases, a tool may support both privacy and security needs (e.g., Tool 23 and 24).
- Each group of tools includes:
  - policy and agreement templates that can be customized for your First Nation
  - planning frameworks that will guide your First Nation through the process of putting plans in place (e.g. incident management or business continuity)
  - letters and forms for use in various privacy situations
  - guides for First Nation Health facility staff – question and answer documents, fact sheets and role descriptions.
- Some of the tools and templates support mandatory legal requirements (such as Tools 4, 7, 10, 13,14,24 and Appendix B).

The results of the assessments in Step 1: ASSESS will help you determine which templates and guides are priorities for your First Nation.

Notable…

Some of the tools and templates support mandatory legal requirements. Other tools provide important information on processes.

Tool #3
Privacy Policy

Instructions

A Privacy Policy sets out how your health facility will protect clients' personal privacy under PHIPA. Staff, contractors, students, and volunteers should be familiar with your Privacy Policy. If asked, clients should be able to view your Privacy Policy.

This is a Privacy Policy template you can use to develop a new policy or update your current policy to meet the privacy needs of your facility. In addition to this policy, each First Nation will need to develop processes and procedures to support their policy.

INSERT YOUR LOGO HERE

Privacy Policy

At <First Nation Health Facility>, privacy is guided by the Personal Health Information Protection Act (PHIPA), a law that establishes rules for the collection, use, and disclosure of Personal Health Information. As a Health Information Custodian (HIC), we and our agents (including staff, contractors, students and volunteers), are responsible for ensuring that the Personal Health Information of our clients is treated with respect and sensitivity. Anyone who collects, uses, or discloses Personal Health Information on our behalf must follow this Privacy Policy.

1: Responsibility for Personal Health Information (PHI)

<First Nation Health Facility> is responsible for the PHI in our custody or control. The <position> has been designated as the Privacy Contact. The <privacy contact> is responsible for assisting <First Nation Health Facility> to follow PHIPA rules through the following activities:

- Applying policies and procedures to protect PHI
- Informing staff, contractors, students and agents about privacy policies and procedures
- Responding to questions and concerns from staff, clients, community members, and leadership
- Reviewing all privacy policies and procedures on a regular basis.

2: Identifying Purposes for Which Personal Health Information is Collected

We collect PHI for purposes related to:

- direct client care;
- managing programs and services
- service planning
- managing the health care system
- statistical reporting
- as permitted or required by law.

We post a Privacy Notice to tell the community our privacy practices and why PHI is collected. We also share this notice through other means such as our website or brochures. We review our Privacy Notice annually to ensure it is up to date.

If PHI that has been collected is needed for a purpose not previously identified, we obtain client consent, unless the new purpose is permitted or required by law.

3: Consent for the Collection, Use, and Disclosure of Personal Health Information

We collect PHI directly from the client or from the person acting on the client's behalf. We rely on implied consent and/or express consent.

Clients may withdraw consent at any time, but the withdrawal cannot apply to past collection, use, or disclosure. PHI will only be disclosed without consent if permitted or required by law.

We make sure that only those people who need to see personal records are allowed to look at them. We further protect information through administrative policies, specific contracts (such as data sharing agreements with external agencies), and by adopting appropriate safeguards and security measures.

4: Limiting Collection of Personal Health Information

We limit the amount and type of PHI collected to only what is necessary for the purposes identified in the Privacy Notice. PHI may include name, date of birth, address, health history, record of visits to a health care provider, and the services received.

Occasionally, we will collect PHI from other sources, if consent has been obtained or if the law permits.

5: Limiting Use, Disclosure, and Retention of Personal Health Information

We limit use, disclosure and retention of PHI to the purposes described in the Privacy Notice. Only those individuals that need to use PHI for direct care or administrative purposes are allowed to access client records. Every employee, contractor, student and volunteer signs a confidentiality agreement to protect PHI within our control Where appropriate, we use information sharing agreements with third parties when PHI is involved.

Personal Health Information is securely and permanently destroyed following the retention period.

6: Accuracy of Personal Health Information

We keep PHI as accurate, complete, and up to date as possible for the purposes it was collected. All client information is recorded following the practice standards of their respective college or professional association. For example, nurses must follow the College of Nurses of Ontario (CNO) Practice Standard: Documentation, Revised 2008 (CNO 2009)[1].

Clients may request a change to their health record by contacting the Privacy Contact.

7: Safeguards for Personal Health Information

We established safeguards for the PHI in our custody or control. Some of the safeguards include:

- Physical measures (such as locked filing cabinets)

[1] College of Nurses of Ontario:Documentation, revised 2008, CNO, 2009: http://www.cno.org/learn-about-standards-guidelines/publications-list/standards-and-guidelines/

- Access policies (such as allowing access to a member of the health team on a "need-to-know" basis)
- Technological measures (such as the use of passwords, encryption, and audits)
- Confidentiality agreements
- Contracts containing privacy requirements (e.g., data sharing agreement)
- Privacy Training.

All staff, contractors, students, and volunteers are required to follow the safeguards. Failure to follow our safeguards and policies may result in disciplinary actions, up to and including termination of employment.

8: Openness about Health Information Privacy and Security Practices

Our health information privacy and security practices for PHI are described in our Privacy Notice. The Privacy Notice is posted for public information.

9: Client Access to Personal Health information

Clients may request access to their PHI. We respond to such requests within 30 days as required by PHIPA.

10: Questions or Concerns about <First Nation Health Facility's> Privacy Practices

Questions or complaints about our Privacy practices and the protection of PHI can be sent to <privacy contact> and/or the Office of the Privacy Commissioner. Contact information is provided in the Privacy Notice and posted for public view.

Tool #4
Responsibilities of a Privacy Contact

Instructions

As a HIC, your First Nation health facility has specific responsibilities under PHIPA regarding the privacy and protection of PHI.

Health facilities must name a Privacy Contact. The role of Privacy Contact can be included as responsibilities of an existing staff member (for example, a Health Director, a Community Health Nurse, a Community Health Representative, etc.) and included in the job description.

Tip

The role description describes the responsibilities of a Privacy Contact.

A full time position as Privacy Contact may not be required.

INSERT YOUR LOGO HERE

Responsibilities of a Privacy Contact

The <First Nation Health Facility> Privacy Contact should be familiar with:

- Applicable First Nation privacy legislation
- PHIPA and privacy principles
- The health facility's privacy policies and procedures
- How to protect individual and community privacy within aggregate information, such as community reports.

The following responsibilities are part of the role of the Privacy Contact at <First Nation Health Facility>.

The Privacy Contact:

- Has an active role in making sure staff follow privacy laws
- Ensures that external contractors or contacts (such as visiting healthcare professionals, students and volunteers) are informed about their privacy responsibilities and the health facility's privacy policies and procedures
- Responds to client questions, complaints, access, and correction requests related to information practices
- Advises the < First Nation Health Facility > about how privacy and security policies, practices, and procedures can be consistent with PHIPA obligations and best practices
- Identifies privacy training, assessment tools, and awareness opportunities for staff
- Investigates and reports privacy and security breaches
- Responds to questions from leadership and management regarding how PHI is managed, protected and disclosed.

Tool #5
Health Information Privacy and Consent: Frequently Asked Questions - Staff

Instructions

This set of Frequently Asked Questions (FAQ's) is appropriate for any health facility staff. You can use this tool with the *Consent for Using and Disclosing Personal Health Information: A Staff Guide* (Tool #9) for a detailed discussion of consent requirements under a variety of disclosure scenarios relevant to these FAQ.

INSERT YOUR LOGO HERE

Health Information Privacy and Consent: Frequently Asked Questions - Staff

1. Is our health facility a Health Information Custodian (HIC) and what does that mean for us?

The Personal Health Information Protection Act (PHIPA) applies primarily to "Health Information Custodians" (HICs) who are named under the Act.

The definition of the HIC includes a centre, program or service for community health or mental health whose primary purpose is the provision of health care. Health facilities are included in this definition, provided that they are operated by First Nations and not the Federal government. Federal government health facilities are subject to the Privacy Act, not PHIPA.

Other HICs include a person who operates:

- A public hospital
- A psychiatric facility
- A long-term care facility, or
- A laboratory.

In these examples, the "person who operates" is typically a Board of Directors or other group with corporate responsibility. For a First Nation health facility, it may be Chief and Council or a Board of Directors.

Other HICs include:

- Health care providers, whether they are regulated (such as nurses and doctors) or unregulated (such as community health representatives and mental health counselors, as long as they are paid to provide health care services, and
- The Ministry of Health and Long-Term Care.

PHIPA has rules for collecting and using Personal Health Information (PHI), for disclosure of information to support client health care services, and for purposes such as health service management and planning. Specific HIC obligations include:

- PHI is only collected, used by or disclosed to those employees or agents who need to know the information to carry out the purpose to which the client consented
- Every collection, use or disclosure of information must be limited to the minimum necessary for the purpose it was collected
- Client consent is required for the collection, use or disclosure of their PHI. The health facility relies on implied or express client consent.

It is important to know which health care providers and organizations are HICs because it affects the way information can be shared (or disclosed). For example, a HIC can rely on a client's implied consent to share their PHI with another HIC who is also involved in the client's care. Express consent is required to disclose PHI with a non-HIC.

Appendix B has a detailed description of HIC's responsibilities under PHIPA.

2. What is PHI?

Personal Health Information (PHI) can be oral (spoken) or recorded (written down). The following list of statements can help you determine whether the information you have is defined as PHI:

- On its own, or if linked to other information, it can be used to identify an individual (including the individual's Certificate of Indian Registry number or "band number")
- It relates to the physical or mental health of an individual, including immunization records and his/her family history
- It relates to the health care an individual has received, or identifies the people responsible for providing health care to that individual
- It relates to the individual's eligibility for coverage for health care
- It relates to payment for health services or medical transportation in a manner that identifies the individual
- It relates to reporting requirements to the Non-Insured Health Benefit (NIHB) program in a manner that identifies the individual
- It relates to the individual's donation of body parts or bodily substances (including their testing)
- It is the individual's health (OHIP) number
- It identifies the individual's substitute decision-maker
- It is part of a record that contains PHI, even if it is not itself PHI. (This is called a "mixed" record, which is covered as PHI under PHIPA.)

If any of the above statements is true, the information is PHI.

3. Can PHI about a client be collected from someone other than the client?

Yes. It is common that someone other than the client will provide health facility staff with PHI about the client. For example, a substitute decision-maker (e.g. Power of Attorney) may provide PHI about an individual, or parents may report information for their children about immunization services administered off-reserve.

HICs may collect PHI indirectly (from someone other than the client) if:

- Consent has been given by the client, or the client's substitute decision-maker
- There is a law that provides authority to the HIC do so
- There is a law that permits or requires another person to disclose the PHI to the HIC
- The PHI is needed to provide care to the client, and there is no other reasonable way to get the information.

4. What is the difference between Implied Consent and Express Consent?

Implied Consent is when HICs assume that a client has given consent to the collection, use or disclosure of his/her PHI for the delivery of health care service or treatment. For example, your family doctor may disclose your PHI to a specialist who is also providing care to you, unless you specify otherwise. The client's willingness to see the specialist implies their consent.

Express Consent is when HICs specifically ask for a client's consent before any collection, use, or disclosure of PHI takes place. Express Consent can be obtained in writing or verbally and should be documented. For example, your express consent is required for your family doctor to provide your PHI to a life insurance company.

5. How do you obtain consent when there is a customary care arrangement or adoption?

PHIPA states that if a person is incapable of consenting to the collection, use or disclosure of their PHI (such as would be the case of a child) there are others who may provide that consent. These individuals include:

- A child or parent of the individual
- A Children's Aid Society
- A person who is lawfully entitled to give or refuse consent in the place of a parent
- A brother or sister of the individual
- Any other relative of the individual.

6. What is the difference between a "use" and a "disclosure" of PHI?

PHI is "used" when it is shared between a HIC and agent, or among the agents of a HIC. For example, if one staff member shares a client's PHI with another staff member providing care to the client, the information is being used. Note that this assumes that the use is consistent with the original purpose of collection and that the client has consented to the collection of PHI for that purpose.

This is different than a "disclosure," which happens when PHI is given to someone who is not collecting, using or disclosing PHI on behalf of the health facility. For example, sharing PHI with a traditional healer operating independently from the health facility is a disclosure and would require the client's express consent.

7. When can PHI be "used" without additional consent?

There are a number of situations in which PHI can be used without the additional consent of the client. PHI can be used for the purpose it was collected, as described in the health facility's Privacy Notice. PHI can also be used without additional client consent for purposes such as health program planning, auditing for program quality, monitoring user access for potential misuse, and information disposal or de-identification. Please refer to Consent for Using and Disclosing Personal Health Information: A Staff Guide (Tool #9) for a detailed discussion of consent requirements.

8. When can PHI be "disclosed" without consent?

There are a number of situations in which a HIC does not have to get client consent to disclose PHI:

- The Personal Health Information Protection Act (PHIPA) or other laws allow or require the disclosure. An example is the mandatory reporting of Adverse Events Following Immunization (AEFI) to public health authorities under the *Health Protection and Promotion Act*

- In proceedings of a court or tribunal
- To designated agencies for planning and management of the health system
- In situations where it is necessary to eliminate or reduce a significant risk of serious bodily harm to the client or to another person
- To assist in a client's placement in a health care facility
- To assist in placing an individual into a custodial setting, such as under the Criminal Code mental disorder provisions.

9. Can a child under 16 give consent regarding collection and disclosure of their PHI?

Generally, the parents or guardians of a child under 16 make consent decisions for their children.

However, a child under 16 is legally entitled to make their own consent decisions provided that the child demonstrates that he/she is making an informed and voluntary decision. The details are covered in the *Health Care Consent Act*, section 11.

As an example, there may be situations where a child under 16 consents to receive an immunization against their parents' wishes. Assuming that the child is able to make an informed decision, staff would be able to act on the child's consent decision.

10. What are my obligations for privacy when carrying out case management?

In general, the use of PHI for case management is permitted under PHIPA. In the event that the health facility is requested to provide information to a Public Health Unit or Board of Health for case management purposes under the Health Protection & Promotion Act, the health facility is required to provide the requested information. This information can be disclosed without client consent.

11. How do I manage records that I take outside of the health facility?

It may be necessary to remove PHI (including paper copies of PHI) from your health facility. The same legal obligations to protect the privacy and security of PHI apply regardless of the location of the records. The Mobile Devices Security Fact Sheet (Tool #20) includes a set of privacy and security tips that may be helpful.

12. Who can I disclose information to when the request comes from outside of the First Nation?

Where organizations such as a Public Health Unit are acting under their legal authority, PHI can be disclosed without the consent of the client or their legal guardian. It is important that the request has a legal authority, for example under the Health Protection and Promotion Act.

13. What is the health facility's obligations regarding agents that may have access to PHI?

PHIPA applies to a HIC's "agents" if they collect, use or disclose PHI on behalf of the HIC. Agents can include:

- Employees and consultants
- Health-care practitioners (if they are acting on behalf of the HIC)
- Volunteers
- Students
- Independent contractors (including physicians and third-party vendors who provide you with supplies or services).

14. Are persons providing traditional healing services or traditional midwifery considered HICs?

No. PHIPA sec 3(4) states the following:

> A health information custodian does not include a person described in one of the following paragraphs who has custody or control of personal health information as a result of or in connection with performing the work described in the paragraph:
>
> 1. An aboriginal healer who provides traditional healing services to aboriginal persons or members of an aboriginal community.
> 2. An aboriginal midwife who provides traditional midwifery services to aboriginal persons or members of an aboriginal community.
> 3. A person who treats another person solely by prayer or spiritual means in accordance with the tenets of the religion of the person giving the treatment. 2004, c. 3, Sched. A, s. 3 (4).

A HIC would require a client's express consent to disclose PHI to a First Nation healer or midwife. Implied consent would not be sufficient under the Act.

If the traditional healer/midwife is an employee or agent of the health facility, then the health facility is the responsible HIC of PHI.

Tool #6
Confidentiality Agreement

Instructions

As the HIC, the health facility must ensure that all staff (including contractors, students and volunteers) that have access to PHI sign a Confidentiality Agreement. If your facility does not have an existing agreement, this tool can be used as is, by inserting the facility name in the spaces indicated, or can be adapted as needed.

INSERT YOUR LOGO HERE

Confidentiality Agreement

I have read and understood <First Nation Health Facility> policies and procedures on privacy, confidentiality and security. I understand that:

- All confidential and/or PHI that I have access to or learn through my work with <First Nation Health Facility> is strictly confidential:
- As a condition of my work with <First Nation Health Facility>, I must follow these policies and procedures: and
- My failure to follow these policies and procedures may result in disciplinary action or termination and may also result in legal action being taken against me by <First Nation Health Facility> and/or others.

I will not access, use or disclose any confidential and/or PHI that I learn of or possess because of my work with <First Nation Health Facility>, unless it is necessary for me to do so in order to perform my duties or where required by law. I also understand that any confidential and/or PHI will not be communicated either inside or outside of <First Nation Health Facility>, except to other persons who are authorized to receive such information.

I will not alter, destroy, copy or tamper with confidential and/or PHI, except with authorization and in accordance with the policies and procedures of the (First Nation Health Facility>.

I agree to keep computer access codes (for example, passwords) confidential and secure. I will protect physical access devices (for example, keys, key fobs and badges) and the confidentiality of any PHI being accessed. I will also protect the security of computer equipment (for example, laptops, memory sticks and other portable devices).

I understand that access codes, access devices and computer equipment come with legal responsibilities and that I am responsible for their use. If I have reason to believe that my access codes, access devices and computer equipment have been lost, stolen, or inappropriately used, I will immediately contact my supervisor or the Privacy Contact at <First Nation Health Facility>.

This agreement will continue to be in effect after the end of any contract that I have with the organization, which means that my obligation to maintain privacy extends beyond the end of my work.

Name: _____

Date: _____

Tool #7
Privacy Notice

Instructions

PHIPA requires the HIC to develop a public document such as a notice, fact sheet, brochure, or poster that describes why PHI is collected, used and disclosed. This notice should include a general description of the administrative, technical and physical safeguards, processes and procedures that are used to protect PHI. It must also tell clients:

- Who the Privacy Contact is and how to get in touch with him/her
- How to ask for access to (and correction of) their health records held by the health facility
- How to inquire about privacy processes and procedures or other matters relating to PHIPA within the health facility
- How to make a complaint to the facility's Privacy Contact or to Ontario's Information and Privacy Commissioner.

You can use the following Privacy Notice as is by inserting the name of your First Nation health facility where indicated, or you can adapt it for your specific needs.

INSERT YOUR LOGO HERE

Privacy Notice

Collection of Personal Health Information

As part of providing quality health services, Personal Health Information is collected, either directly from clients or from the person acting on their behalf. Personal Health Information collected by the <First Nation Health Facility> may include, name, date of birth, address, health history, record of visits, and the services received. Occasionally, <First Nation Health Facility> will collect Personal Health Information from other sources, if consent has been obtained or if the law permits.

Use and Disclosure of Personal Health Information

To provide quality health services, Personal Health Information may be used or disclosed to:

- Communicate with health care providers including family doctors and/or other health care institutions to care for clients (unless the <First Nation Health Facility> is otherwise instructed)
- Manage internal <First Nation Health Facility> plans, operations, and risk-management activities
- Manage performance and quality improvement activities (such as sending client satisfaction surveys)
- Follow legal and regulatory requirements
- Fulfill other purposes permitted or required by law.

The <First Nation Health Facility> limits access to client records and Personal Health Information to only authorized personnel that require the information to provide direct client care or for health administrative purposes. The <First Nation Health Facility> further protects information through administrative policies, procedures, and security measures.

To Access or Correct Your Information

Clients may view or obtain a copy of their health record maintained at <First Nation Health Facility>. If a client believes that their Personal Health Information at the <First Nation Health Facility> is inaccurate or incomplete, the client can write to request a correction. Please contact <name of privacy contact person, First Nation Health Facility, address, other contact information>.

For More Information

For more information or to raise questions or complaints about privacy and information practices, please contact: <name of contact person, name of First Nation Health Facility, address, other contact information>.

Complaints about information and privacy practices can also be made to the Provincial Information and Privacy Commissioner at: Information and Privacy Commissioner/Ontario, 2 Bloor Street East, Suite 1400, Toronto, Ontario M4W 1A8, Tel: (416) 326-3333 or Toll-free: 1-800-387-0073.

Tool #8
Health Information Privacy and Consent: Frequently Asked Questions - Clients

Instructions

This set of FAQs contains information on health information privacy and consent that can be shared with clients, community members, First Nation leadership, and health facility staff for reference and educational purposes.

INSERT YOUR LOGO HERE

Health Information Privacy and Consent Frequently Asked Questions - Clients

1. What is Privacy?

Privacy is your right to decide what information is collected about you, how it is used, and to whom it is disclosed (shared or released). Protecting privacy means keeping information both "confidential" and "secure".

Confidentiality in a health care setting is making sure that information given to a health care provider, as part of receiving care, is not disclosed to anyone unless needed to provide your care.

Security of Personal Health Information requires keeping it safe and having controls in place to protect confidentiality. Examples include using passwords to access computers, proper storage of clinical files, locked doors, and policies and procedures.

2. What is Personal Health Information?

Personal Health Information (PHI) is information about you as an individual, either spoken or written and can include:

- Physical or mental health history, including a family health history
- The health care provided to the person, including the name of their health care provider
- A plan of service for the person
- Eligibility for health care coverage
- A lab test, or the donation of a body part or substance
- A health card number
- The name of a substitute decision-maker.

PHI can be combined to create summary reports about groups of people. Summary reports are used when individual information is not required, such as program planning.

3. What is Consent?

Consent is the permission that a person gives for the collection, use, or disclosure (sharing) of his/her PHI, as described in the Privacy Notice.

4. When do I Give Consent?

You will be asked to give your consent when we have initial contact with you. We will also ask for your consent when health information is requested for use or disclosure to someone other than direct health care providers or as permitted by law.

5. Can I refuse or withdraw consent?

Yes. You have the right to refuse or withdraw your consent. You can withdraw consent at any time. However, withdrawing consent will not affect PHI that has already been collected, used, or disclosed.

6. How does the health facility protect the privacy of my Personal Health Information?

The <First Nation Health Facility> is responsible for your PHI in our custody or control. We have a Privacy Contact who manages privacy and security procedures. Privacy, security, and the confidentiality of PHI is protected through:

- Following policies and procedures to protect your PHI
- Ensuring that only authorized personnel are allowed to look at PHI
- Informing staff, contractors, students, and agents about privacy and security policies and procedures
- Responding to questions and concerns
- Reviewing all privacy and security policies and procedures on a regular basis.

Everyone who works in the health facility is required to respect the privacy rights of our clients. Our Privacy Notice and Privacy Policy are available.

7. What law protects the privacy of my Personal Health Information?

If a First Nation community has developed their own health information privacy laws, these will apply to your PHI. For First Nations that do not have their own laws, the Personal Health Information Protection Act (PHIPA) is legislation that controls the privacy and security of Personal Health Information in Ontario. PHIPA includes rules about collection, use, or disclosure of PHI and clients' rights to give, refuse, or withdraw consent.

8. Who owns my Personal Health Information?

You, as the client, own the PHI contained in the health record. Your PHI is stored in a health record created by the health facility that delivers the health services.

9. Who owns the record containing my Personal Health Information?

The health facility that delivers your health services has a professional and legal obligation to keep a record (digital or paper) of the services provided to you. Clients own their Personal Health Information and can request to see a copy of their records.

10. Can I change or correct my health record?

If you believe there is an error or omission, you can request that your information be added.

11. Who can see my Personal Health Information?

Your PHI can only be accessed, used or disclosed with others that directly provide health care to you, the people that support your direct providers, and to others as required or allowed by the Personal Health Information Protection Act (PHIPA).

12. Can I choose who sees or does not see my Personal Health Information outside of the health facility?

You can permit others to see your PHI by giving consent, and you can withdraw consent at any time.

13. What happens to my Personal Health Information if I no longer use services at this health facility?

If you move or decide to stop receiving health care services at the health facility, you may request a copy of your health records for your new health care provider. We will keep a copy of your records, which is a legal and professional requirement. We will destroy archive records in accordance with health industry standards.

14. How is my Personal Health Information kept secure at this health facility?

We take many steps to make sure that your PHI is secure and protected. Some of these safeguards include:

- Physical measures (such as locked filing cabinets)
- Organizational measures (such as allowing access to information on a "need-to-know" basis only)
- Technological measures (such as the use of passwords, encryption, and audits).

15. Who can I contact if I have additional questions about the privacy of my Personal Health Information?

Privacy Contact at <First Nation Health Facility>
<ADDRESS>
<PHONE NUMBER>
<E-MAIL>

You can also contact the Privacy Commissioner of Ontario at:

Information and Privacy Commissioner / Ontario
2 Bloor Street East, Suite 1400
Toronto, ON M4W 1A8
Telephone: 416-326-3333 or 1-800-387-0073
Email: info@ipc.on.ca
Website: www.ipc.on.ca

Tool #9
Consent for Using and Disclosing Personal Health Information:

A Staff Guide

Instructions

You can use this guide to consistently manage client consent for the collection, use, and disclosure of PHI. This guide does not address consent concerning provision of health services.

You will find a list of steps involved in consent management, a description of key parts of consent, and other information to assist your staff to meet legal and professional requirements.

This guide also includes a number of specific examples that will assist staff in handling situations involving the use or disclosure of PHI:

- **Consent Examples: Use of PHI:** A table of examples identifying when no additional consent is required for use of PHI
- **Consent Examples: Disclosure of PHI:** A table of examples identifying the kind of consent required in different situations for disclosure of PHI, e.g. implied consent, express consent, no consent.

INSERT YOUR LOGO HERE

Consent for Using and Disclosing Personal Health Information

A Staff Guide

Steps in Consent Management

These are the general steps when managing situations involving client consent:

1. Check to see that this is a situation in which consent is involved, which means that there is a collection, use or disclosure of PHI.
2. Understand the elements of valid consent.
3. Identify who needs to give consent, and ensure the person is capable of giving consent
4. Determine what type of consent needs to obtained. Refer to the Consent Examples for Use and Disclosure of PHI tables below.

What is Consent?

Consent is the permission that a person gives for the collection, use, or disclosure of his/her PHI. To be valid under PHIPA, the consent:

- Is granted by the individual (or of the appropriate substitute decision-maker, if there is one).
- Is based on the client having knowledge about what they are consenting to, which can also be achieved by posting a notice of the health facility's information practices). This is also known as "informed consent".
- Relates to the information being collected.
- Is not obtained through deception or coercion.

Clients should understand that they can choose not to give consent, or if given, they can withdraw consent at any time.

When is Consent Required?

Consent is only required when dealing with Personal Health Information (PHI). PHI is identifying information about an individual in oral or recorded form, if the information is:

- About the physical or mental health of the individual, including information that consists of the health history of the individual's family
- About the provision of health care to the individual, including the identification of a person as a provider of health care to the individual
- Is a plan of service (as defined by the Long-Term Care Act, 1994) for the individual.
- About payments or eligibility for health care in respect of the individual

- About the donation by the individual of any body part or bodily substance of the individual or is derived from the testing or examination of any such body part or bodily substance
- Is the individual's health number
- Identifies an individual's substitute decision-maker.

For First Nations, a Band Number can also be PHI if it used to uniquely identify clients for the provision or management of health care.

Who will give the consent?

A capable person has the right to make his/her own decisions about the collection, use, and disclosure of PHI.

If a client has a substitute decision-maker entitled to make decisions under the *Health Care Consent Act*, this person automatically becomes the substitute decision-maker under PHIPA for information decisions related to the client's PHI.

If a client does not have a substitute decision-maker for treatment and is incapable of making decisions about the collection, use or disclosure of his/her PHI, staff must turn to the list of substitute decision-makers in PHIPA. (See below for further detail about capacity determinations and list of substitute decision-makers.)

a) Consent of a capable person

The general rule under PHIPA when obtaining consent is that it must be the consent of a capable person. The test of whether or not a person is capable relates to:

- His/her ability to understand the information that is relevant to making a decision about the collection, use, or disclosure of PHI
- The ability to appreciate the probable results ("reasonably foreseeable consequences") of giving or not giving, withholding, or withdrawing the consent.

b) Consent on behalf of an incapable person

If there are any doubts about a client's capacity, staff should proceed to determine his/her capacity. A "Determining Capacity to Provide Consent Form" (Tool #13) is available for this purpose.

PHIPA provides a ranking of substitute decision-makers who have the right to give, withhold, or withdraw consent on behalf of an incapable person:

- The individual's guardian of the person or guardian of property (if the guardian has authority to make a decision on behalf of the individual)
- The individual's attorney for personal care or attorney for property (if the attorney has authority to make a decision on behalf of the individual)
- The individual's representative appointed by the Consent and Capacity Board (if the representative has authority to give the consent)
- The individual's spouse or partner

- A child or parent of the individual, or a Children's Aid Society or other person who is lawfully entitled to give or refuse consent in the place of the parent. This paragraph does not include a parent who has only a right of access (visits) to the individual. If a Children's Aid Society or other person is lawfully entitled to consent in the place of the parent, this paragraph does not include the parent
- A parent of the individual with only a right of access to the individual
- A brother or sister of the individual
- Any other relative of the individual.

The Public Guardian and Trustee have discretion to act as the substitute decision-maker only if no one in the list above can fulfill this role.

In a customary care situation, the customary care-giver would be able to provide consent based on their role as a substitute decision-maker under one of the categories in the above list.

The client may challenge the finding of incapacity to the Consent and Capacity Board.

Types of Consent: Express versus Implied Consent

Consent may either be express (written or oral) or implied. However, as identified in the examples below, there are a few circumstances where the consent cannot be implied, and staff must obtain express consent. There are also some use and disclosure situations when additional client consent is not required, as noted in the examples.

Implied Consent occurs when Health Information Custodians (HICs) assume that an individual has given consent to the collection, use or disclosure of his/her PHI for the delivery of health care service or treatment. For example, several nurses in your health facility may share PHI when each is involved in providing care to the client. Each provider in the "circle of care" is relying on implied consent.

Express Consent occurs when HICs specifically ask for an individual's consent before any collection, use, or disclosure of PHI takes place. Express Consent can be obtained in writing or verbally. For example, express consent is required for a family doctor to provide PHI to a life insurance company.

When obtaining a client's express consent, it is important that it be documented. This could be a written consent signed by the client, or a staff member recording the fact that the client gave oral consent. Staff must also follow any standards for documentation of their professional college, other licensing body or their health facility.

Consent Examples: Use of PHI

The table below contains uses and examples of PHI when additional client consent is **not** required.

Use of PHI – Additional Consent Not Required	
Uses of PHI – A Guide These examples all assume that a client consented to the initial collection of PHI. HICs or their agents can use PHI without further client consent for the following things:	
For the purpose for which the PHI was collected and all functions related to that purpose	Example: Updating a client's immunization record Exception: HICs cannot use PHI if the client initially consented but then withdrew their consent; or if the PHI was collected indirectly from someone other than the client and the client tells the HIC not to use it
For risk management.	Example: Confirming a client's immunization history prior to administering a vaccination
For activities to improve the quality of the health facility's programs or services	Example: Conducting data quality audits to ensure that staff are documenting care properly
To get consent from a client	Example: A HIC can use client information to contact a client in order to obtain or confirm consent to use PHI
For purposes of disposing of the PHI or to de-identify the PHI	Example: Using a shredding company to dispose of PHI
To share PHI with staff to provide better care to clients	Example: Two nurses discussing the health of a client currently receiving care in the health facility. They are both involved in that care
To plan or deliver programs or services to clients.	Example: Preparing a client list for an upcoming HPV clinic
To monitor for misuse	Example: Performing an audit of a user's activity when there has been a concern of accessing PHI inappropriately
To obtain payment for health care services	Example: Administering payment for medical transportation reimbursement
If the health facility or staff are involved in a proceeding (or anticipated proceeding) before a court or tribunal, such as a Consent and Capacity Board; at an inquest; or as part of a professional college's review of a member's	Example: A staff member has been called before the College of Nurses of Ontario disciplinary committee regarding alleged negligence in administering immunizations

Use of PHI – Additional Consent Not Required	
Uses of PHI – A Guide These examples all assume that a client consented to the initial collection of PHI. HICs or their agents can use PHI without further client consent for the following things:	
conduct, such as a physician, psychologist, nurse or social worker	
To educate agents to provide health care	Example: Training a new or student health care provider in the use of a health information system
For any other purpose allowed under PHIPA, or another law or treaty.	Example: Reporting an instance of a reportable disease.

Consent Examples: Disclosure of PHI

The following checklist is helpful in determining the kind of consent required for various situations. This set of examples is based on PHIPA. Where First Nations have developed their own privacy legislation, those requirements should be referenced.

All examples involve PHI, unless specifically noted.

Even if a HIC is entitled to rely on implied consent in the examples below, they may choose to obtain the express consent of the client.

In the Table below, a check mark (✓) indicates the form of consent required for each example.

Consent for Disclosure of PHI Scenarios						
Disclosure From	Disclosure To	Purpose	Consent Required		No Consent Required	PHIPA Reference
			Implied	Express		
HIC	HIC	Providing health care			✓	38.(1)(a)
HIC	Agent of HIC	Providing health care			✓	38.(1)(a)
HIC	Non-HIC[2]	Providing traditional health services		✓		18.(3)(a)
HIC	Non-HIC	Other than providing health care		✓		18.(3)(b)
HIC	HIC	Other than providing health care		✓		18.(3)(b)
HIC	Agent of HIC	Other than providing health care		✓		18.(3)(b)
HIC	Client	Client request		✓		right of access

[2] Non-HIC includes Traditional healers and Traditional midwives providing traditional services to First Nation people

Consent for Disclosure of PHI Scenarios						
Disclosure From	**Disclosure To**	**Purpose**	**Consent Required**		**No Consent Required**	**PHIPA Reference**
			Implied	**Express**		
HIC	Band administration	Other than providing health care		✓		18.(3)(b)
HIC	As required	Protect the health or safety of the individual or others			✓	40.(1)
HIC	As required	Required by law			✓	41.(1)
HIC	As required	Identify a deceased person or provide reasonable notice of a person's death			✓	38.(4)(a)
HIC	As required	Provide reasonable notice of a person's death			✓	38.(4)(b)
HIC	As required	For the individual's spouse or family to make decisions about their own or their children's health care			✓	38.(4)(c)
HIC	MOHLTC / LHIN / HIC	Determine funding or payment			✓	38.(1)(b)
HIC	As required	Contact a relative or friend when individual is unable to provide consent			✓	38.(1)(c)

Consent for Disclosure of PHI Scenarios						
Disclosure From	**Disclosure To**	**Purpose**	**Consent Required**		**No Consent Required**	**PHIPA Reference**
			Implied	**Express**		
HIC	Head of Penal or Custodial Institution or an officer in charge of a psychiatric facility where the patient is being lawfully held	Assist in decision making regarding health care or placement			✓	40.(2)(3)
HIC	HIC's potential Successor	Assess or evaluate HIC's operations			✓	42.(2)
HIC	HIC's Successor	Notice must be given before or after disclosure			✓	42.(2)
HIC	HIC	Determine or verify eligibility for health care			✓	39.(1)(a)
HIC	HIC	Conduct or review an audit or accreditation			✓	39.(1)(b)
HIC	HIC	Compile or maintain a PHI registry			✓	39.(1)(c)
HIC	Chief Medical Officer	For the purposes of the Health Protection and Promotion Act, e.g. to report a communicable disease			✓	39.(2)(a)

Consent for Disclosure of PHI Scenarios						
Disclosure From	**Disclosure To**	**Purpose**	**Consent Required**		**No Consent Required**	**PHIPA Reference**
			Implied	**Express**		
HIC	Public Health Ontario	For the purposes of the Ontario Agency for Health Protection and Promotion Act			✓	39.(2)(b)
HIC	Public Health Authority	For the purposes of the Health Protection and Promotion Act, e.g. to report a communicable disease			✓	39.(2)(c)
HIC	Individual assessing patient capacity, who is not providing care to the patient	Determine, assess or confirm capacity under the Substitute Decisions Act, Health Care Consent Act, or Personal Health Information Protection Act			✓	43.(1)(a)
HIC	Fundraiser	Fundraising		✓		32.(1)
HIC	Researcher	Research purposes using PHI (dependant on a research plan and approval from applicable Research Ethics Board)[3].			✓	44.

[3] Note that the HIC must obtain the express consent of the client for the researcher to contact the client directly.

Consent for Disclosure of PHI Scenarios						
Disclosure From	**Disclosure To**	**Purpose**	**Consent Required**		**No Consent Required**	**PHIPA Reference**
			Implied	**Express**		
HIC	Panorama	To transfer immunization charts from current system to Panorama. Note: This would apply for any format of historical immunization records (i.e. computer application/database, or hard copies of client charts).			✓	PHI has already been collected
HIC	Panorama	To populate the First Nations Attribute screen for clients who have existing immunization records with the First Nation health facility			✓	PHI has already been collected
HIC	Panorama	To pre-populate the First Nation Attribute screen for all members of the First Nation, to help determine immunization coverage rates, etc.			✓	Not PHI - PHIPA does not apply

Consent for Disclosure of PHI Scenarios						
Disclosure From	**Disclosure To**	**Purpose**	**Consent Required**		**No Consent Required**	**PHIPA Reference**
			Implied	**Express**		
HIC	Unspecified	Release of aggregate information reports that do not identify individuals			✓[4]	Not PHI - PHIPA does not apply
Federal Health Facility	Unspecified	Release of aggregate information reports that do not identify individuals. Note: Federal Health Facilities are subject to the Privacy Act, not PHIPA			✓	Privacy Act Applies; no restriction on aggregate data

[4] Although PHIPA does not require consent for the release of aggregate information, First Nations need to decide how community aggregate information may be shared outside the First Nation.

Consent for Disclosure of PHI Scenarios						
Disclosure From	**Disclosure To**	**Purpose**	**Consent Required**		**No Consent Required**	**PHIPA Reference**
			Implied	**Express**		
HIC	College of a regulated health care professional	Where there are reasonable grounds to believe a health care professional has sexually abused a patient, details of the allegation, name of the health care professional and name of the allegedly abused patient will be shared. Note: the patient's name can only be provided with consent. You must also include your name as the individual filing the report.			✓	Regulated Health Professions Act

Consent for Disclosure of PHI Scenarios						
Disclosure From	**Disclosure To**	**Purpose**	**Consent Required**		**No Consent Required**	**PHIPA Reference**
			Implied	**Express**		
HIC	College under the Regulated Health Professions Act, or Social Work and Social Services Act, or Board of Regents under the Drugless Practitioners Act	Administration/ enforcement of the relevant statutes			✓	43(1)
HIC	Order, warrant, writ, summons or other process issued by an Ontario court	Information outlined on the warrant, summons, etc.			✓	41(1)
HIC	Subpoena issued by an Ontario court	Information outlined in the subpoena			✓	41(1)

Consent for Disclosure of PHI Scenarios						
Disclosure From	**Disclosure To**	**Purpose**	**Consent Required**		**No Consent Required**	**PHIPA Reference**
			Implied	**Express**		
HIC	Researcher, research organizations or Universities	Analyze or compile statistical information. Research must be conducted under a research plan submitted to the HIC, that a prescribed research ethics board has approved, in accordance with PHIPA.			✓	O.Reg. 18(1)
HIC	Public Guardian and Trustee	Investigate an allegation that a patient is unable to manage their property			✓	43(1)
HIC	Public Guardian and Trustee (PGT), Children's Lawyer, Residential Placement Advisory Committee, Registrar of Adoption of Information, Children's Aid Societies	Carry out their duties and, for the PGT, to investigate serious adverse harm resulting from alleged incapacity			✓	43(1)

Consent for Disclosure of PHI Scenarios						
Disclosure From	**Disclosure To**	**Purpose**	**Consent Required**		**No Consent Required**	**PHIPA Reference**
			Implied	**Express**		
HIC	Lawyers, Insurance Companies, Adjusters, Investigators on behalf of a third party, if the third party is an agent or former agent of the HIC	Assist the third party with a proceeding			✓	37(1), 41(2)
HIC	Investigator or Inspector	Conduct an investigation or inspection authorized by a warrant or law			✓	
HIC	Police without a warrant	Where there are reasonable grounds to believe that the disclosure is necessary for the purpose of eliminating or reducing a significant risk of serious bodily harm			✓	43(1)

INSERT YOUR LOGO HERE

Tool #10
Consent to Disclose Personal Health Information: General Consent Form and Immunization Data Consent Form

Instructions

If staff at your health facility are asked to share client information with a third party, you can use the consent checklist (Tool #9) to assist in determining whether written consent to disclose PHI is required.

This tool contains two templates for written consent:

- 10a Consent to Disclose Immunization Information
- 10b Consent to Disclose Personal Health Information (General Consent)

These forms are not to be used for consent for treatment.

Tool #10a
Consent to Disclose Immunization Information

Instructions

This Consent for Disclosure form is designed only for requests to disclose immunization information.

Consent to Disclose Immunization Information

INSERT YOUR LOGO HERE

I, _____ hereby consent to disclosure / sharing of

(Print your name)

☐ all information OR ☐ partial information (specify): _____

contained in the <First Nation Health Facility's> immunization record to:

_____

(Name of Individual / Agency to Receive Information)

Concerning: _____ _____

(Client Name) (Your relationship to Client)

Date of Birth: _____

For the purpose of: _____

_____

Return Consent (Complete this section if the receiving individual/agency will be returning or sharing information back to the health facility).

This consent further authorizes: _____

(Individual / Agency Name)

To disclose information contained in the record of: _____

(Client Name)

to <---First Nation Health Facility's--->, for the above noted purpose.

This consent remains in effect, unless withdrawn by me in writing.

_____ _____

(Signature) (Witness)

Dated this _____ day of _____ , _____

(Day) (Month) (Year)

Tool #10b
Consent to Disclose Personal Health Information

Instructions

This following Consent for Disclosure form is designed specifically for requests to disclose personal health information

INSERT YOUR LOGO HERE

Consent to Disclose Personal Health Information

I, _____ born _____, authorize _____

(Print your name) (Date of birth) (Print name of Health Information Custodian)

to disclose ☐ my personal health information consisting of:

_____

_____

(Describe the personal health information to be disclosed)

or ☐ the personal health information of:

_____

_____

(Name and address of person for whom you are the substitute decision-maker*)

consisting of _____

_____

(Describe the personal health information to be disclosed)

to _____

_____

(Print name and address of person receiving the personal health information)

I understand the purpose for disclosing this personal health information to the person named above. I understand that I can refuse to sign this consent form.

My Name: _____

Signature: _____ Date: _____

*Please note: A substitute decision-maker is a person authorized to disclose personal health information on behalf of:

_____

(Name of person for whom you are the substitute decision-maker)

Tool #11
Personal Health Information Inventory

Instructions

As part of the HIC role, the First Nation health facility needs to manage details of PHI in its custody. This form can be used to track details about where PHI is located and who has access to make management easier and faster in the event of a privacy breach.

Tool #19 is provided to manage IT Assets.

Tip

The information in this tool can be used to generate reports that can assist you in managing the PHI of your clients. This tool is available in both Word and Excel format.

INSERT YOUR LOGO HERE

Personal Health Information Inventory

The following list describes the types of information in the Personal Health Information Inventory.

Type of Information	Description	Instructions for Recording this Information
Folder Name	The name of the folder containing PHI.	The folder name should be identified as either a: • Filing cabinet • Electronic folder If electronic, provide the full location description. (filing cabinet, directory and subfolders for electronic files)
Location	The place where the PHI is accessed or stored.	List all locations and devices where PHI is stored. Provide any locations where PHI can be Accessed or Stored, using the category titles: • Access • Store
Media Type	Describe the PHI format.	Values for the PHI format include: • Paper • Electronic • Film
Description	Provide a brief description of the PHI.	Examples: Files containing Referrals, Diagnostic Imaging, Dietician reports.
Access by	The roles that can have access to the PHI.	Provide the roles in the health facility include: • Physician • Nurse • Etc.
Status	The extent to which the record currently is in use.	Statuses for PHI records include: • Active • Inactive • Transferred • Archived • Destroyed
Status Change Date	Date when record changes status.	Provide the date where the status changes. The date should be in the format YYYY-MM-DD. If the record is active and there has been no change in status, this field should be blank, otherwise it should be populated.

PHI Inventory

Folder	Location	Media Type	Description	Access by:	Status	Status Change Date
Examples: p:/ClinicRecords/OutPatient/DieticianAssessments/2012	Access: Clinic #1 & #2 Stored: Server 4	Electronic	Dietician Assessment Notes from 2012	Physicians, nurses	Active	
n:/ClinicalRecords/WellBabyUltrasounds/2012	Access: Clinic 1 Stored: Server 1	Electronic	Well Baby Clinic Assessments from 2012	Physicians, nurses	Active	
Paper Discharge Files 1995	Access: Reception, Clinic #1 and #2 Stored: Filing Cabinets in Unit ABC	Paper	Discharge Information – 1995	Physicians	Archived	2006/3/31

Personal Health Information Inventory
Health Facility Name

Folder	Location	Media Type	Description	Access by	Status	Status Change Date

Tool #12
De-Identifying Personal Health Information

Instructions

There will be times when your health facility is asked to prepare reports or answer questions. It is important that these reports or answers not contain PHI or information that could be used to identify individuals. All information that could identify an individual should be removed to protect their privacy.

You can use this Tool to consider the situations where you will have to de-identify PHI.

INSERT YOUR LOGO HERE

De-Identifying Personal Health Information

What is Identifiable Information?

PHIPA defines "identifiable information" as information that lets you identify an individual based on the PHI you have about their health or health care. PHIPA says this includes when information could be used *either alone or with other information*, to identify an individual.

PHIPA defines personal information as *identifiable information* about a person in oral or written form that relates to:

- their physical or mental health
- the health care provided to them
- payments or eligibility for health care coverage
- the donation of body parts or substances
- a plan of service under the Long-Term Care Act
- is the individual's health card number, or
- Identification of an individual's substitute decision-maker.

In some cases, information from different sources can be combined to identify an individual. For example, in a small community, information about a client's health condition may be combined with their band number or the date that a blood test was done, and this might be enough information to identify the client.

Why Do I need to De-identify Information?

HICs have a responsibility to de-identify PHI as much as possible. The goal is to protect the individual's privacy by preventing direct identification or linking information to breach the client's privacy.

How Do I De-Identify Information?

The following actions can be used to help reduce the risk of client identification:

1. Where possible, remove personal identifiers (such as name, date of birth, etc.)
2. Identify and, where possible, remove additional information that may also identify a client (such as marital status, health card number, band number, etc
3. Replace personal identifiers with random identifiers. For example, client names could be replaced with random names or references such as "Client XYZ"
4. If small numbers of examples are recorded, include these in a larger, more general category so the clients cannot be singled out and identified. (For example, if you have only two pregnant teens in a small community, report these as part of all pregnant women in your region to reduce the chance the teens will be identified)

5. use data sharing agreements that commit the receiver to use the information only for specified purpose, not re-identifying the information, and not to combine the shared information with information from other sources

Examples: When to De-Identify PHI

The following examples explain when de-identification is required or should be considered "best practice":

1. The health facility treats clients with substance abuse problems. First Nation Management or Leadership asks the health facility for a report about patterns of substance abuse in the community, with categories for age ranges, gender, and type of substance being abused.

   Privacy considerations: Although client names were not requested, age ranges and gender could be used in small communities to identify clients. If there is a risk that clients could be identified, information must be further de-identified, for example: combining age groupings.

2. In a First Nation community, the Chief and Council provide management oversight of the First Nation health facility. An annual planning meeting is coming up, and the nurse has been asked to help leadership plan for next year's programs by providing details about client use of health programs.

   Privacy considerations: PHIPA allows PHI to be used for health planning purposes, however, the nurse should consider whether PHI is really required for this purpose. If data is combined, thought should be given to whether other information (such as age ranges or gender) might be used in small communities to positively identify clients. If possible, always use de-identified information.

3. A client has received partial doses of vaccines over the years and now wants her immunizations brought up to date. The nurse is unsure about the best strategy for doing the catch up and wants to send the client's immunization history to the FNIHB-OR Zone Nurse for advice.

   Privacy Considerations: The information is being used for the purpose of providing care to the client, which is consistent with the informed consent provided by the client. The name of the client is not necessary for the consultation, although age and gender may be significant. The name should be replaced with an anonymous identifier (e.g., Client XYZ).

Tool #13
Record of Assessment:

Determination of Capacity to Provide Consent

Instructions

At times you may be required to make a clinical decision regarding the ability (or capacity) of a client if a client's capacity is in question. Their capacity should be assessed by a health professional, and the results of that assessment recorded in the client's file. Such situations may include when your client has a mental disability or memory impairment, or is a minor child.

You can use Tool 13 for recording the details of a capacity assessment.

INSERT YOUR LOGO HERE

Record of Assessment:

Determination of Capacity to Provide Consent

An individual is capable of giving consent to the use and/or disclosure of their PHI if he/she is able to:

1. Understand relevant information about whether to consent to the collection, use or disclosure
2. Appreciate the reasonably foreseeable consequences of giving, not giving, withholding or withdrawing their consent.

The above considerations apply to clients regardless of age, including children under age 16.

Completed by: _____

(Staff Name)

_____

(Staff Title)

Client's Full Name: _____

Client's Date of Birth: _____

Client Identifier: _____

Meeting Date with Client: _____

Assessment Outcome: _____

_____

_____

_____

_____

Signature of Assessor: _____

Tool #14: Request Form for Personal Health Information Review & Decisions

Instructions

This tool is a form that you can use to record the details of a client request to:

1. View their health record
2. Change or amendment of information in their health record, or
3. Receive or send a copy of their health record.

This form will also assist your health facility to record the decisions made in response to client requests to view or request changes to their PHI.

Notable…

This form is not intended to capture details about the routine exchange of information between health facilities.

INSERT YOUR LOGO HERE

Health Record Access and Change Request Form

Date Request Received: _____ (YYYY/MM/DD)

Request Number: _____ (Optional)

A. Contact Information			
Name of Requestor:		Requestor Phone #:	
Requestor Email:		Requestor Mobile Phone #:	
Requestor Address:			
Complete Name of Client:		Client Date of Birth:	
Client Address:		Client Health Card Number or Band Number:	

B. Request for Copy/Amendment of Client Record	
Separate Written Request Received:	☐ Yes (attach) ☐ No (complete section B)
Type of Request: ☐ Copy Request ☐ Amendment Request	☐ Laboratory Report ☐ Surgical Report ☐ Other diagnostic report (specify): ☐ Outpatient Report: ☐ Clinic Report (Specify Clinic): ☐ Consultant Report (Specify consultant):
Reason for Request:	
☐ Specific date requested. Please specify: (YYYY/MM/DD) ☐ Date Range requested. Please specify: (YYYY/MM/DD – YYYY/MM/DD)	
Provide record to: ☐ Requestor ☐	Contact Details:

Third Party		
If the requestor is not the client, has Consent to Disclose Personal Health Information been granted? ☐ Yes ☐ No		
Is the client requesting correction to an error? ☐ Yes ☐ No ☐ Unknown		
Describe the error if known:		
Requestor: (Signature and date)	(Signature)	(YYYY/MM/DD)
To be completed by the health facility		
C. Decision and Response (required within 30 days of the original request)		
Final Decision:	☐ Request Approved. Record reviewed by requestor. ☐ Request Approved. Record updated to include new information. ☐ Request Approved. Copy of Record provided to requestor or third party. ☐ Access request Declined. **Reason:** ☐ Requestor does not have a right of access ☐ Investigation or legal proceeding planned or underway ☐ Risk of harm to self or others ☐ Access would identify a third party informant ☐ Other reason	
Requestor Notified: (date notified)	☐ (YYYY/MM/DD)	
Authorized by: (signature and date)	(signature)	(YYYY/MM/DD)

Tool #15
Security Policy

Instructions

This is a Security Policy template to assist health facilities to manage the security of the PHI in their control. This tool will need to be customized according to the organizational structure within your community.

This tool contains a comprehensive list of responsibilities to be considered for security, however, these items can be adjusted based on the needs and capacity of the health facility.

INSERT YOUR LOGO HERE

Security Policy

1. Purpose / Policy Objectives

The <First Nation Health Facility> is dependent in many ways on both information and information systems. If sensitive information is unavailable, unreliable, or disclosed improperly, the health facility and its clients could suffer serious harm or loss. This may also impact the reputation of the health facility. For these and other reasons, <First Nation Health Facility> has implemented an information security program which includes this Security Policy.

2. Involved Persons

To be effective, information security must be a team effort. It involves the participation and support of every staff member, contractors, students and volunteers who deal with sensitive information and information systems. This policy identifies the responsibilities of all users and the steps they must take to help prevent and respond to different types of threats to information and information systems. Such threats include unauthorized access, disclosure, duplication, modification, appropriation, destruction, loss, misuse, and denial of use.

All staff, contractors, students and volunteers must treat the <First Nation Health Facility's> security measures as confidential and must not divulge these security measures to clients or external individuals.

3. Involved Systems

This security policy deals primarily with computer and network systems used, owned or administered by <First Nation Health Facility>. It applies to all platforms (operating systems), all computer sizes (from personal digital assistants through to servers), and all software (whether developed by the health facility or purchased from third parties). There are some safeguards mentioned that apply to the security and safety of paper and other physical records.

4. Security Program Roles and Responsibilities

4.1. Health Information Custodian

HICs are accountable for the privacy and security of PHI and community-related health data that is collected, used, disclosed or retained by the health facility. This responsibility may be delegated for the protection of PHI and community-related health data to facility staff.

4.2. Health Lead (e.g. Health Director)

The Health Lead has overall management responsibility for the following:

(a) Day-to-day application of reasonable security management measures to protect against the unauthorized access, collection, use, disclosure, retention or disposal and integrity of PHI

(b) Ensure that all employees, contractors, students and volunteers are informed of the security procedures and understand their responsibilities for protecting PHI and critical information systems

(c) Ensure that security incidents within the health facility are investigated and appropriate corrective actions taken

(d) Ensure approval of privacy and security policies and procedures

(e) Manage requests for physical access to premises

(f) Manage requests to enable and disable access to systems

(g) Review user roles and access privileges at least once a year to ensure that they are still appropriate for each user's job function

(h) Ensure that background reference checks are performed on individuals prior to granting user access to secure areas or systems

(i) Ensure that security responsibilities are included in the terms and conditions of employment, service contracts, or volunteer activity

(j) Ensure that all users have signed the Acceptable Use Policy form.

The security management process follows the requirement for appropriate separation of duties. For example, the person requesting access to PHI cannot be the person approving the request.

4.3.IT Support Personnel or Designated Individuals

The roles and activities of the designated IT support personnel or designated individuals include:

- Act with "Administrator" privileges on all computers. Ensure that end users do not have Administrator privileges unless authorized by management.
- Manage the security of the computer network and infrastructure.
- Ensure that a record is kept of users that have keys or pass codes for secure areas. Audit sign-in or entry records for secure areas.
- Ensure that a record is kept of all information and information technology assets.
- Enable and disable user accounts on direction from management. In particular, accounts must be disabled within 24 hours of the end of the user's relationship with the health facility.
- Ensure that firewalls are used on portable devices and dedicated internet links (ADSL, Cable).
- Manage all computer equipment installations, disconnections, modifications, repairs, servicing and relocations, and secure disposal.
- Ensure that users back up data on personal computers and laptops, including documents, contact lists, and email messages. All backups containing critical or confidential information must be stored at an approved off-site location with physical access controls or encryption.
- Ensure that all software used in the health facility is appropriately licensed.

- As applicable, ensure that Virtual Private Network (VPN) Split tunnelling is disabled.
- Ensure that current virus detection software is installed on all technology assets including mobile devices, operating correctly, and configured to automatically update daily.
- Identify the encryption tools to be used when PHI is stored on laptop computers, and for secure transmission by email. Assist staff with the use of encryption.
- Ensure that software is updated on a regular or automatic basis. In particular, recommended security patches are installed for the operating system and other applications in use.
- Monitor the computer network logs for unauthorized access, viruses, spyware and other security breaches.
- Ensure that all user access to systems is automatically logged with the user's login name, date and time of access, the system / application accessed and the action taken.
- Ensure that computer access logs are securely saved for a minimum of two years.
- Ensure that clinical files are archived in accordance with the health facility's policy for data retention.
- Investigate any alleged misconduct in consultation with management and the Privacy Contact. All investigations will be performed on a case-by-case basis.
- Document procedures for key business processes such as system backup and restore, software upgrades, patch management, etc.

5. Physical and Access Security

Access to every office and room in the health facility that contains confidential (non-public) information is physically restricted only to people who have a need to know. The following specific measures are required of all staff, contractors, students and volunteers:

- All computers and portable devices (e.g., laptops and cell phones) that access the network and/or data must be password protected.
- Laptop computers must be secured with locking cables to avoid risk of theft.
- Automatic password protected screen savers must be used with timeout periods appropriate to the sensitivity of the data being accessed (For example, the more sensitive the information, the faster a screen saver should activate during periods of inactivity).
- Computers must not be left logged on when unattended.
- Any computer device displaying confidential information must be positioned out of public view.
- Users must ensure that confidential information is not left unattended on desks or on computer screens unless the doors and windows are locked.
- Any printer or fax machine used to send or receive PHI should be kept in a closed area to prevent unauthorized persons from seeing the documents.

- Authorized users will be given keys or door pass codes to allow access to secure areas of the health facility.
- Key computer system components have battery backup to protect equipment and information if there is a power failure.
- End users are not provided with Administrator privileges on any computer system, with the exception of Authorized Support Personnel and any individuals authorized by management.

6. User IDs and Passwords

Each staff member, contractor, student, or volunteer accessing health facility computer systems has a unique user identification (user ID) and a private password. User IDs are used to limit access to the system based on the job duties of each user. Each worker is personally responsible for his or her user ID and password.

6.1. User Accounts are Personal and Private

Computer system user accounts are personal to each authorized user. There are no shared accounts. Users may not access computers or networks anonymously, such as by using "guest" user IDs. Inappropriate use of passwords includes:

- Sharing passwords without management approval
- Writing passwords down in any way or through email
- Storing an unprotected password in a file on any computer system.

Users must not use the "Remember Password" feature of any software application (e.g. Internet Explorer).

If a user suspects that their password has been discovered, they must report it to their direct supervisor and change the password immediately.

To minimize the risk of unauthorized access and maintain password confidentiality, user passwords should be easy to remember but hard for others to guess. Passwords must not be related to the user's job or their personal life. For example, the following should not be used as passwords: the user's address, spouse's name or licence number, or single words including names, places, slang words or technical terms.

Users must **not** create passwords with a basic sequence of letters that is then partially changed based on a date or other predictable factor. For example, users must not use "JAN2013" in January and then change the password to "FEB2013" in February. Users must also not create passwords that are the same as or similar to passwords they have used before.

6.2. Strong Passwords

Use of strong passwords is required, using the principles below. As much as possible, these controls are managed automatically:

- Passwords automatically expire every 3-6 months. Users are required to change their passwords as follows:

- To prevent password recycling, users are not able to reuse any of their previous eight passwords
- Temporary passwords must be changed on the first log-on

- User accounts are locked out after five failed log-on attempts within a 45-minute period
- The shortest acceptable password length is 8 characters
- The password must contain characters from three of the following four categories:
  - English uppercase characters (A – Z)
  - English lowercase characters (a – z)
  - Base 10 digits (0 – 9); and
  - Non alphanumeric (For example: !, $, #, or %).

7. Release of Information

Unless it has been specifically designated as *public* information, all information maintained in the health facility must be protected from disclosure. This includes client demographic data (such as name and address), contractual and employment information, and data in summary form (such as immunization coverage reports). All release of information (except public information) must be approved. Such information releases may include questionnaires, surveys and interviews, but does not include client requests for access to their own information or a person for whom they are a substitute decision maker.

8. Network Infrastructure Security

Only authorized devices will be permitted to access the network. Personal devices such as usbs, iPods and iPads must not be connected to the network without management approval. Network devices connected to the computer network must not be modified, disconnected or relocated without management approval.

Wireless access points, peer-to-peer wireless connections and Wi-Fi devices must not be installed within a facility without management approval.

9. Internet Access

Staff, contractors, students and volunteers may be provided with internet access. Such access may be terminated at any time at the discretion of management. The health facility monitors internet use to ensure that workers do not visit internet sites unrelated to their work, and to monitor for potential security issues.

Specific authorization is required in advance for workers to:

- Represent the health facility in internet discussion groups or other forums
- Posting any health facility information (including public information, photos of health facility events, comments or posts) to the internet (such as Facebook) without management approval.

All information received from the Internet should be treated cautiously unless the source has been confirmed to be reliable.

10. Electronic Mail

Health facility workers who use computers for their work are given an email address. All email communication on behalf of the health facility must use this assigned email address. Email accounts created on behalf of the health facility must be approved by and are the property of the health facility.

Use of personal email addresses for health facility purposes is not permitted unless formally authorized. Staff must use a standard email "signature" (authorized by management) that includes their full name, job title, address and phone number, along with a privacy statement. Email use is for health facility purposes only and is monitored.

Sound judgment must be used when distributing messages. Carbon copy (Cc) and Blind carbon copy (Bcc) distribution options should be used only as necessary to support the actions identified in the email message. Client-related messages should be carefully guarded and distributed to only the essential people. Staff must also abide by copyright laws, ethics rules, and other applicable laws.

Confidential information must not be sent via e-mail unless encrypted by approved encryption software and procedures. This includes the transmission of PHI, financial information, employee records, or other confidential material.

Only authorized management personnel are permitted to access another person's e-mail without consent.

11. Computers, Laptops, Peripherals and Mobile Device Security

The following security measures apply to use of computer equipment:

- Users must observe all manufacturers' instructions for protecting computer devices. Computer equipment and portable storage devices must be kept away from hazards such as direct sunlight, liquids, high or low humidity, extreme heat or cold, smoke, vibration, chemical effects, electrical supply interference and magnetic fields.
- Users should avoid drinking beverages or eating food around computer equipment.
- Only authorized support personnel are permitted to service computer devices.
- All computer equipment must have proper physical security mechanisms in place (i.e. be protected by key locks and cables and/or alarms) if left unattended or in open areas.
- When not in use, any computing device (computer, laptop, peripheral, mobile device) or media must be stored in a securely locked and hazard free location.
- PHI must be encrypted if stored on laptops or other mobile devices.
- Users must ensure that data on personal computers and laptops is backed-up (or that authorized support personnel at the health facility are taking care of this requirement). All backups containing critical or

confidential information must be stored at an approved off-site location with physical access controls or encryption.

12. Remote and Mobile Usage

Users must adhere to the following requirements for remote and mobile use of computer equipment:

- Personal mobile devices must not be connected to the network without management approval.
- Users must not take portable devices or media off the premises of the health facility without the informed consent of their immediate supervisor. Informed consent means that the supervisor knows what equipment is leaving, what data is on it and the purpose for its use.
- Remote access to the network, applications, and data is for business purposes only. Health facility management must approve all remote access to PHI.
- Log in passwords must be used on all remote-computing devices.
- Users must not use the "Remember Password" feature of any software application (e.g. Internet Explorer).
- Computers and mobile devices supplied by the health facility must not have their hardware or software configuration changed in any way without management approval. Only authorized support personnel are permitted to make configuration changes.
- Computers and mobile devices must be logged off, locked, or shut down completely when not in use. The automatic log off must be set to run after a short period of inactivity.
- All portable laptops, notebook computers and mobile devices, including storage media, must use standard encryption technology when used to carry personal identifiable information or other confidential electronic data.

If a user is unsure about how to comply with these requirements, they must contact their immediate supervisor or authorized support personnel.

13. Network Threats and Malicious Code from External Sources

All users are responsible for following security protocols while accessing the computer network and services to protect the health facility against viruses, worms, Trojan horses and other malicious code. The following security measures are required of all staff, contractors, students and volunteers to minimize these threats:

- All software installation must be authorized.
- Users must not knowingly allow malicious code such as spyware, worms, viruses or other software that may cause a threat to the network to be installed on the health facility's computers.
- Before use, users must scan all portable storage media (including CDs, DVDs, and media sticks) that are new or are of unknown origin for viruses.

- The downloading or installing of any files is not permitted unless authorized. This includes (but is not limited to) software programs, screen savers, music and video files from the internet.
- Any user who suspects that his/her workstation has been infected must immediately power off the workstation and call authorized support personnel. Users must not attempt to destroy or remove malware, viruses, spyware and/or other Internet born security threat, or any evidence of them, without direction from authorized support personnel.
- Users must immediately report any signs or suspicions of computer or network tampering, intrusions, or security breaches to their direct supervisor and authorized support personnel.
- If any computer device is damaged, lost or stolen, the user must immediately notify their direct supervisor and follow the Privacy and Security Incident Response Plan (Tool 22).

Failure to follow this policy will result in temporary or permanent suspension of access to the network and may lead to disciplinary action up to and including termination, cancellation of contractual arrangement, as well as civil and criminal action.

14. Right to Search and Monitor

Health facility management or authorized agents have the right to monitor, inspect, or audit all facility information systems. Such an examination may take place with or without consent, or the knowledge of involved workers. The information systems subject to examination may include among others:

- Email files
- Hard drive files
- Voice mail files
- Printer files
- Fax machine printouts
- Desk drawers and filing cabinets.

Workers should have no expectation of privacy regarding information stored in or sent through health facility systems.

Audits may be performed:

- In response to a complaint or concern
- In response to a trigger from system monitoring software
- On a random basis.

15. References

- Privacy and Security Incident Response Plan (Tool 22)

Tool #16
Business Continuity Management Plan

Instructions

The Business Continuity Management Plan (BCP) helps you plan how your health facility will operate following a "disaster" or disruptive event (such as fire, flood, power disruptions, information system failure, etc.). BCP involves establishing business continuity and disaster recovery plans for services, clients, and staff.

A BCP plan is needed to support the health facility's response to events that can happen in any department of your organization. As such, the scope of a BCP plan is considerably broader than a single eHealth project, such as Panorama. Many communities may already have a plan in place as part of their Emergency Preparedness Plan (EPP).

This tool outlines the privacy and security-related elements of a Business Continuity / Disaster Recovery Plan. Many communities will know this as an Emergency preparedness Plan. This tool is not a Business Continuity / Disaster Recovery Policy but provides a checklist of key information required to create or update your BCP.

INSERT YOUR LOGO HERE

Business Continuity Management Plan

What is BCP?

The Business Continuity Management Plan helps plan how an organization will continue its business following a disaster or disruptive event. Many communities have a plan in place known as an Emergency Preparedness Plan (EPP). Examples of such emergency events include fire, floods, power disruption, information system failure, illness that affects large numbers of people, etc. BCP involves establishing business continuity and disaster recovery plans for services, clients, and staff. The contents of this document are the key items that <First Nation Health Facility> will need if a disruptive event occurs.

Establish Business Continuity Support

A successful BCP requires a coordinator, active support from a BCP team, and input from key individuals from across the organization. These functions may already exist in your health facility as part of your Emergency Preparedness Plan.

The **BCP Coordinator** is a person already working within <First Nation Health Facility> who organizes the plan, takes direction from a BCP team, and works with different members of <First Nation Health Facility> to ensure that departments across the organization participate and contribute to the plan.

The **BCP Team** provides strategic direction and guidance for the BCP process, approving BCP-related policies. Each health facility will identify who should be part of the BCP team, but the Health Director, Chief, and other senior leaders are typically included.

Key Individuals represent the different business areas of <First Nation Health Facility>, acting as contacts for planning purposes and as leaders when a disruptive event happens.

The people involved in BCP at <First Nation Health Facility> are:			
Name	**Title**	**Department**	**Contact Information**
BCP Coordinator			
BCP Team			

The people involved in BCP at <First Nation Health Facility> are:			
Name	**Title**	**Department**	**Contact Information**
Key Individuals			

Reference Documents for BCP

In the event of a disruptive event, it is important to be able to review the health facility's business areas and confirm the impact of the event to those areas. The following documents need to be compiled, kept up to date, and held in a single location for easy reference by the BCP Coordinator following a disruptive event:

BCP Documents Referenced During Disruptions		
The following BCP Documents can be found at <location of BCP document>:		
Document Updated?	**Document Name**	**Description**
☐	First Point of Contact List	A list of the most up to date information for key staff to be contacted in the event of a disruption. This list would include phone number (work, home & mobile), email and physical address.
☐	Roles and number of staff	The Roles and Number of Staff in Tools 1 & 2 (Privacy and Security Assessments) help confirm all staff are accounted for and are part of the communication plan. It also is used to plan the roles that are required to remain at work or return to work following the event.
☐	Asset Management Inventory	Tool #19 is used to identify important IT assets that need to be brought back online, restored or replaced.

BCP Documents Referenced During Disruptions		
The following BCP Documents can be found at <location of BCP document>:		
Document Updated?	**Document Name**	**Description**
☐	Personal Health Information Inventory	Tool #11 is used to track the PHI in the HIC's custody. This list is used to manage information if a privacy breach occurs. It can also be used to locate information quickly if the health facility needs to issue a response (or report) to an event that requires PHI, such as a pandemic.
☐	Privacy & Security Incident Report Plan	Some incidents cause the BCP to be put into effect. Tool #22 lists the steps for responding to incidents.
☐	Privacy & Security Incident Reporting Form	Tool #23 lists the details about an incident that needs to be gathered. These details may assist in resolving the incident and will help to identify ways to prevent future similar incidents.
☐	List of Emergency Backup Systems	A list of backup systems to cover power or utility failures.
☐	Procedures for Data backup and restore	Procedures for routine data backup and restore.

Tool #17
Access to Network Services Request Form

Instructions

This tool is a form that you can use to record the details of requests for access to your health facility's network services.

You may wish to revise this form to include the types of system access that may be requested by your health facility. Requests recorded on this form should be kept by IT staff or the person responsible for information security. It is recommended that the form be completed any time there is a requested change to the user's network services.

INSERT YOUR LOGO HERE

Employee Access to Network Services Request Form

Request Number (optional): _____

A. User Information			
Name:		Department:	
Email:		Position:	
Phone #:			

B. Access to Network Services			
Service Name	Configuration Details/Access Rights (e.g. for role-based access)	Start Date (YYYY/MM/DD)	End Date (YYYY/MM/DD)
Network Access			
Clinical Management System			
Panorama			
Internet			
Email			
Community Lab Access			
Remote Access			

D. Approval Signature(s)		
Approved by:	Signature of Approver	Date (YYYY/MM/DD)
To be completed by IT		
Implemented by:	IT Signature:	Date (YYYY/MM/DD)

Tool #18
Acceptable Use Policy

Instructions

You can use this tool to inform employees, contractors, students and volunteers about acceptable use guidelines when accessing the First Nation health facility's electronic systems and services. This tool should be used together with your Security Policy.

Users should review and sign the Acceptable Use Policy prior to any access of systems and services. By signing the Acceptable Use Policy, users are agreeing that they have read and understand the Acceptable Use, Privacy, and Security Policies. This is important to protect the health facility from inappropriate use of electronic systems and services and to help users clearly understand what they can and cannot do. If this policy is used, it is important that that staff, contractors, students and volunteers sign this form in the same manner as the Confidentiality Agreement.

Two versions of this tool are provided. Each health facility should choose the most appropriate one for their needs:

1. Internet Acceptable Use Policy: This covers just user access to and use of the health facility's Internet service. It does not cover E-mail, Network and Software use.
2. Electronic Services Acceptable Use Policy: This is a broader policy that covers E-mail, Internet, Network and Software use. This policy applies to users who will access Panorama.

Acceptable Internet Use Policy Statement

<First Nation Health Facility> recognizes that many employees, contractors, students and volunteers need to have access to the Internet while working. Therefore, we make the Internet available for health facility purposes.

<First Nation Health Facility> specifically bans its employees, contractors, students and volunteers from accessing the following types of sites using health facility computers and mobile devices ([… revise list based on local policy …]):

- Social Networks (e.g. Facebook)
- Gaming sites
- Gambling sites
- Auction sites (e.g. eBay)
- Movie or video programming sites (e.g. Netflix)
- Hate sites
- Pornographic sites
- Any site engaging in or encouraging illegal activity

<First Nation Health Facility> may use monitoring software to make sure the Internet Acceptable Use Policy (IAUP) is being followed. We may record and/or monitor computer and Internet activity for any reason and without notice.

By signing and dating this document:

- You agree that you have reviewed this document and had the opportunity to ask questions.
- You agree to follow the <First Nation Health Facility> IAUP.
- You agree to follow the <First Nation Health Facility> Privacy Policy and the Security Policy
- You agree that if you do not follow the IUAP, Privacy Policy, and Security Policy, you will be subject to disciplinary measures by <First Nation Health Facility>, including possible termination.

Acknowledgement of Receipt and Understanding

I hereby state that I have read and understand the contents of the Internet Acceptable Use Policy and the Security Policy. I acknowledge that <First Nation Health Facility> reserves the right to change or update its policies at any time, with notice.

Signature:

Print Name:

Date:

Electronic Services Acceptable Use Policy

1. General

<First Nation Health Facility> recognizes that many employees, contractors, students and volunteers need access to an e-mail system, a network connection, Internet/Intranet access, and computer software while working. We makes various electronic services available for health facility purposes.

This policy covers all use of electronic services including the e-mail system, network, Internet/Intranet access, and computer software (at all health facility service delivery locations and offices). These electronic services are intended only for <First Nation Health Facility>'s business use. Employees are not permitted to access these electronic services for personal use.

All information created, sent, or received using <First Nation Health Facility>'s electronic services is the property of <First Nation Health Facility>. Users should have no expectation of privacy regarding this information. We reserve the right to access, read, review, monitor/audit, copy all messages and files on any of our computer system(s) at any time and without notice. When deemed necessary, we reserve the right to disclose text or images to law enforcement agencies or other third parties without the user's consent.

The Security Policy includes additional information regarding the security obligations of employees, contractors, students and volunteers. Users should review and understand the Privacy Policy and the Security Policy.

2. Personal Responsibility

By accepting an account, User ID, and password for any electronic service you agree to follow the policies regarding their use. You also agree to report any misuse or policy violation(s) to your supervisor or <First Nation Health Facility>'s Privacy Contact.

3. Banned Activities

Employees, contractors, students and volunteers are banned from using <First Nation Health Facility>'s electronic services for the following activities:

Downloading software without the prior written approval of Authorized Support Personnel.

Sending or forwarding a message that discloses PHI, employee records, or any other confidential information without the approval of management or direct supervisor.

Printing or distributing copyrighted materials. This includes, but is not limited to, software, articles and graphics protected by copyright.

Operating a business, soliciting money for personal gain, or otherwise engaging in commercial activity.

Searching for outside employment.

Making, sending or forwarding defamatory, offensive or harassing statements, including statements based on race, aboriginal status, colour, religion, national origin, ancestry, disability, age, sex, or sexual orientation.

Sending or soliciting sexually oriented messages or images.

Sending ethnic, sexual-preference or gender-related slurs and/or jokes via e-mail.
Attempting to access or visit the following types of sites (<… revise list based on local policy …>):

- Social Networks (e.g. Facebook)
- Gaming sites
- Gambling sites
- Auction sites (e.g. eBay)
- Movie or video programming sites (e.g. Netflix)
- Hate sites
- Any site engaging in or encouraging illegal activity
- Any site featuring pornography, terrorism, espionage, theft, or drugs.
- Engaging in unethical activities or content.

Participating in activities, including the preparation or dissemination of content, which could damage <First Nation Health Facility>'s professional image or reputation.

Permitting or granting use of an email or system account to another employee or person not associated with the health facility.

Using another employee's password or impersonating another person while communicating or accessing the Network or Internet.

Introducing a virus, harmful component, corrupted data or the malicious tampering with any of <First Nation Health Facility>'s computer systems

4. E-Mail Policies and Procedures

<First Nation Health Facility>'s e-mail system is designed to improve service to our clients and partners, enhance internal communications, and reduce paperwork. E-mail system users must follow the policies and procedures below:

Use extreme caution to ensure that the right e-mail address is used for the right recipient(s).

Staff must use a standard email "signature" (authorized by health facility management) that includes their full name, job title, address and phone number, along with a privacy statement.

Personal e-mail accounts may not be used for any health facility purposes unless specifically authorized in advance.

Email accounts created on behalf of the health facility must be approved by and are the property of the health facility.

E-mail messages must contain professional and appropriate language at all times.

Chain messages should be deleted immediately without sending on to others.
With the approval of management, employees may use e-mail to communicate confidential information internally to those with a need to know. Such e-mail must be clearly marked "Confidential."

Employees should save e-mail messages as directed by policy.

5. Network and Internet Policy

Use of the Network and the Internet is a privilege, not a right. We reserve the right to suspend access at any time, without notice, for technical reasons, possible policy violations, security or other concerns. <First Nation Health Facility>, at its sole discretion, will determine what materials, files, information, software, communications, and other content and/or activity will be allowed or banned.

Users may have access via the network to PHI, employee records, financial information and other confidential information. All access to such information must be authorized and used only for First Nation health facility purposes.

6. Software Usage Policies and Procedures

Employees are to use software strictly as allowed by the license agreement. Unless allowed by the license, the duplication of copyrighted software (except for backup and archival purposes by designated <First Nation Health Facility> personnel is a violation of copyright law and breaks our standards of employee conduct.

To ensure the software license agreements are honored, employees must follow the following:

Employees must use software as stated in the manufacturer's license agreements. <First Nation Health Facility> does not own the copyright to software licensed from other companies. Employees acknowledge they do not own this software or its related materials.

<First Nation Health Facility> does not approve and bans the unauthorized duplication of software. Employees illegally reproducing software may be subject to civil and criminal penalties including fines and imprisonment.

If an employee is required to use software at home, we will purchase an additional copy or license as required by the software manufacturer. Any employee issued additional copy(s) of software for home use agrees that additional copy(s) or license(s) purchased for home use are the property of <First Nation Health Facility>.

Under no circumstances will <First Nation Health Facility> use software from an unauthorized source, including, but not limited to, the Internet, home, friends and/or colleagues.

7. Compliance

Each user is responsible for his/her own actions, and our management personnel are responsible to ensure users follow this policy.

Any employee who is aware of a policy violation should immediately report this to their supervisor or <First Nation Health Facility>'s Privacy Contact.

Employees who violate this policy and/or use <First Nation Health Facility>'s electronic services for improper purposes will be subject to disciplinary action, up to and including termination.

Acknowledgement of Receipt and Understanding

I hereby agree that I have read the Electronic Services Acceptable Use Policy, the Privacy Policy, and the Security Policy and fully understand the contents. I have had the opportunity to discuss the information contained in these policies and any concerns that I may have. I understand that my employment is based in part upon my willingness to follow these policies. I agree that <First Nation Health Facility> reserves the right to change or update its policies at any time, with notice.

Signature:	
Print Name:	
Date:	

Tool #19
Information Technology Asset Management Inventory

Instructions

It is important that health facilities track and manage their information and IT assets. There are two main types of assets you need to manage:

- Information Assets, such as health records, in both electronic and paper form. Information Assets include PHI, as well as other types of information that are not considered PHI but are still important to your Health Organization, such as financial reports and operating plans.
- IT Assets, such as hardware and software.

This tool addresses the management of IT Assets. It provides an Asset Management Inventory that can be used as is or adapted for your Health Organization. Tool #11 is provided to manage PHI Assets.

Having a process and a tool for documenting information about assets is a Best Practice for HICs. An Asset Management Inventory acts both as a planning tool and a daily operations tool for managing Information Assets. You can use an Asset Management Inventory to track information about:

- What IT Assets your Health Organization holds
- Key information about assets
- Who is using each asset

This tool was created in Word format. You can also create this tool in Microsoft Excel or Microsoft Access, which have the ability to create reports if you. If your Health Organization uses software such as Excel, Access or Asset Management Tracking software, track your assets in those tools as it is easier to update and manage the information.

INSERT YOUR LOGO HERE

Information Technology Asset Management Inventory

The following list describes the types of information in the Asset Management Inventory.

Type of Information	Description	Instructions for Recording this Information
Asset Name	The word or phrase used to describe the asset.	E.g. Clinic Room #1 Monitor or Health Director Monitor
Asset Type	Describes a category for the asset to assist with identifying who should have responsibility for the asset.	Category types are: • Hardware • Software • Laptop • Other Mobile Device
Date of Arrival	The date the asset arrived at the organization.	Record the date using the YYYY/MM/DD format to assist in sorting the information (if necessary).
Serial Number	The serial number assigned to the asset by the manufacturer	
Make	The name of the manufacturer of the asset.	
Model	The name used for the design or style of the asset as provided by the Manufacturer.	
Location	The place where the asset is used or stored.	Provide a written description of the location. Use “Mobile” if the asset is a mobile device.
User(s)	Who uses this asset at the Health Organization?	It may be an individual or a group of users. Record names of users if possible.

Asset Management Inventory

Asset Name	Asset Type	Arrived on (Y/M/D)	Retired on (Y/M/D)	Serial Number	Make	Model	Location	Users
Example: computer monitor	Hardware	2010/08/30	2012/12/31	1358696	HP	H627DR	Room 2, Outpatient Clinic	Community health nurses (M. Atleo; R. Lalonde)

Tool #20
Mobile Devices Security Fact Sheet

Instructions

This fact sheet provides information to improve security when using mobile devices such as smart phones, laptops, tablets and USB keys. It includes a "Privacy Tips" list with a summary of key points. These tips are intended as an introduction to protecting PHI in a mobile workplace. Check the user manual for each mobile device for further information.

Health facilities may want to revise the "Tips" based on their approved security policy.

INSERT YOUR LOGO HERE

Mobile Devices Security Fact Sheet
Protecting Your Personal Health Information

Mobile devices such as smart phones, laptops, tablets and USB keys offer convenience; however, they may also raise risks for privacy and the protection of PHI. They are also at risk of threats such as viruses and spyware. Staff who have access to, and control of, PHI have a responsibility to protect the privacy of information stored on their mobile devices**.** The following tips can reduce the privacy risks associated with use of mobile devices:

Tips for Protecting Privacy when using Mobile Devices	
1	Learn how to enable privacy and security settings on your mobile device.
2	Only store PHI on your mobile device if it is absolutely necessary.
3	Ensure that mobile devices are protected with hard-to-guess passwords.
4	Use an automatic lock feature so a password is required to access information.
5	Use encryption technology to provide added protection.
6	Install, run, and keep up-to-date anti-virus, anti-spyware, and firewall programs on mobile devices..
7	Don’t send PHI over public wireless networks – for example, at coffee shop hot-spots. Public wireless networks may not be secure and there is a risk that others may be able to capture information sent over these networks.
8	Keep mobile devices in sight. Never leave a mobile device unattended in a public place or a vehicle.
9	Keep laptops locked. Use a laptop security cable to make it difficult for someone to steal it. Make sure to attach the security cable to an immovable or heavy piece of furniture.
10	Ensure that information stored on a mobile device is destroyed before the device is discarded.

Tool #21
Faxing Personal Health Information
Fact Sheet

Instructions

You can use this tool to guide how your health facility discloses PHI by fax. This fact sheet includes a notice that you can post at your fax machine.

INSERT YOUR LOGO HERE

Faxing Personal Health Information Fact Sheet

Faxing personal information increases the risk that it will fall into the wrong hands.

What are the risks?

- A wrong fax number could accidentally be dialed, sending information to the wrong person.
- If a receiving fax machine is unattended, PHI may be viewed by unauthorized individuals.

How can the risks be reduced?

- Consider whether using a fax is the best way of sending confidential information. Is it possible to send the information via courier or another method of secure file transfer?
- Confirm that the receiver has taken steps to prevent anyone else from seeing the faxed documents.
- Before sending a fax:
    - Check that the receiver's number is correct
    - Verify in the machine's display window that the number has been keyed correctly. Better yet, program frequently-used numbers and clearly label the speed-dial keys.
- Use a fax cover sheet clearly identifying both sender and intended receiver. The cover sheet should include:
    - A Privacy Notice
    - Short description of the document(s)
    - Total number of pages the recipient should receive.
- Call the recipient to verify that he or she received the complete transmission and has removed the pages from the fax machine.
- Any fax machine used to send or receive PHI should be kept in a closed area to prevent unauthorized persons from seeing the documents.
- Don’t leave confidential documents unattended. Consider making one person responsible for the fax machine. Otherwise, clinic staff should send their own faxes to limit the chances that others will see PHI. Staff should arrange a time to receive faxes containing PHI so they can be at the machine as the faxes arrive.
- If possible, set up the fax machine so that the receiver has to enter a password before the document will be printed. This ensures that only the intended receiver can retrieve the document.
- If a client asks for his or her PHI to be faxed elsewhere, explain how faxing PHI on can result in accidental disclosure or interception.

Fax Cover Page with Confidentiality Notice

INSERT YOUR LOGO HERE

The fax cover sheet should include a notice that the material contained in the fax is confidential.

Sample Fax Cover Page

To:		From:	
Date:			
Phone Number:		Phone Number:	
Fax Number:		Fax Number:	
Number of Pages (including cover page)			
☐ For Information ☐ For Action ☐ For File ☐ Please Respond			
Comments			
The information contained in this facsimile transmission is privileged and confidential and is intended for the use of the individual named above and others who have been specifically authorized to receive it. If you have received this communication in error, or if any problems occur with transmission, please notify the sender immediately. Thank you for your assistance and cooperation.			

Fax Machine Notice

INSERT YOUR LOGO HERE

Before you send personal information by FAX…

- ☑ **Is FAX the best way to send the PHI, or is there a more secure method?**
- ☑ **Did you check the receiver's FAX number to make sure it's correct?**
- ☑ **Did you complete all the information on the FAX cover sheet?**
- ☑ **Did you verify that you entered the receiver's FAX number correctly?**
- ☑ **Did you call the receiver to let them know that a FAX is being been sent?**
- ☑ **Once sent, have you removed all PHI from the FAX machine?**

Tool #22
Privacy and Security Incident Response Plan

Instructions

This tool provides a basic Privacy and Security Incident Response Plan. You can use this tool to assist your health facility to manage real or potential breaches or incidents.

INSERT YOUR LOGO HERE

Privacy and Security Incident Response Plan

Introduction

Privacy and Security incidents can occur in spite of a HIC's best efforts to protect PHI.

The term "incident" includes both privacy and security events that have the potential to negatively impact or compromise confidential information. An incident includes both suspected and actual incidents; as well as intentional and unintentional. When the incident involves PHI, there may also be a PHIPA breach. Examples of incidents are contained in the table below.

A "PHIPA breach" is a type of incident that occurs when PHI is used or disclosed in a way that breaks the HIC's privacy obligation under PHIPA section 12(1):

> "A health information custodian shall take steps that are reasonable in the circumstances to ensure that personal health information in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal."

Purpose

The Privacy and Security Incident Response Plan will:

- Assist the health facility to respond quickly and effectively to an incident;
- Clearly define staff roles and responsibilities
- Provide an effective investigation process
- Limit potential damages resulting from any breach or incident
- Make it easier to address any breach or incident and
- Prepare the health facility to work with the Information and Privacy Commissioner, if required.

A Privacy and Security Incident Response Plan depends on key individuals:

1. An assigned Privacy Contact and others as required, such as information security and IT personnel; and
2. Health facility management for the overall Incident Response Process.

Examples of Incidents

The following are some examples of incidents that are also PHIPA breaches (note that all PHIPA breaches are incidents):

- Unauthorized collection of PHI (information is collected without consent or legal authority);
- Unauthorized use of PHI, such as looking at a health record out of curiosity;
- Unauthorized disclosure of PHI through:

- loss (a file is misplaced),
- theft (a laptop is stolen), or
- mistake (a letter addressed to one person gets faxed to the wrong person); and

- Unauthorized or unsecured disposal of PHI (an unshredded file is left in the garbage).

The following are also examples of general incidents:

- Employee information is released without authorization;
- Unauthorized release of community summary reports (such as immunization coverage reports);
- Leaving sensitive information unattended on a desk or on-screen;
- Neglecting to have new staff sign Confidentiality Agreements;
- Unauthorized posting of health facility information or pictures on social networking sites;
- Software piracy, copyright abuse, system or application hacking, virus attacks.

Response to an Incident or Breach

All health facility staff, students, volunteers, and contractors must report any suspected privacy or security incidents to the health facility management or Privacy Contact. The report may be done verbally initially but is to be followed up in writing or by e-mail.

Incidents must be handled immediately to minimize the potential privacy impact.

The following are general steps for responding to an incident or breach:

Step 1: Respond to the incident	
☐	When an incident is witnessed, staff will notify the following individuals: (***PRIVACY CONTACT; MANAGEMENT CONTACT***).
☐	The Privacy Contact completes Section A, B and C of the Incident Reporting Form (Tool 23).
☐	Where the incident involves a PHIPA breach, the Privacy Contact and the health facilities' management will decide if the Information and Privacy Commissioner of Ontario (IPC) should be contacted. The Privacy Contact will inform the IPC about the privacy breach and work together with IPC staff.

☐	Contact the Ministry of Health and Long-Term Care if the PHIPA breach involves Panorama. There may be other organizations that need to be notified, such as Health Canada or professional colleges/associations. If the breach appears to involve theft or other criminal activity, notify police. Notify the health facility's insurers if required by the insurance policy. Contact with outside organizations must be authorized by the Health Director.
Step 2: Contain the incident	
☐	Immediate actions must be taken to contain the incident and to limit its impact. Appropriate actions will depend upon the nature of the incident and may include: Isolate or suspend the activity that led to the incident; Stop the unauthorized practice; Correct the weakness in physical or electronic security; Take immediate steps to recover the information, records or equipment from all sources; Revoke or change computer access codes; Determine if any copies have been made of confidential information and recover.
Step 3: Notify individuals as necessary	
☐	Identify individuals whose privacy was breached and notify them of the breach. In the case of a breach involving sensitive First Nation aggregate information, the First Nation leadership should be notified. This can be by letter, phone or other communication method. A sample letter for a personal privacy breach is included in this Toolkit (Tool #24). When giving notice: Provide details of the breach Provide details of the confidential information involved Tell the affected clients of the steps that have been taken or will be taken For a PHI privacy breach, inform the client/management that the Information Privacy Commissioner, the contact for the Ministry of Health & Long-Term Care for Panorama. There may be other organizations that need to be notified, such as Health Canada or professional colleges/associations.

Step 4: Investigate & Address	
☐	Lead an internal investigation and identify the causes for the incident/breach. For example, there may have been a training gap that led to a User accessing PHI inappropriately.
☐	Complete Section D of the Incident Reporting Form.
☐	Submit the Incident Reporting Form to (***MANAGEMENT BODY***) within 10 days of identifying the incident/breach.
☐	For a personal privacy breach, share findings and actions with the Information Privacy Commissioner, the contact for the Ministry of Health & Long-Term Care for Panorama and other organizations identified in STEP 3.
☐	For a personal privacy breach, assist with any further investigation by the Information Privacy Commissioner.
☐	Complete corrective actions to reduce the chance of the incident happening again by the following two steps: Step 1: Set up processes to track and improve incident management and response times Step 2: Train staff about the incidents to make future identification and prevent more effective.

Tool #23
Privacy and Security
Breach Investigation Report

Instructions

This tool is a form that you can use to record the details of an investigation of an actual or potential privacy or security breach. This tool can be used with the Privacy and Security Incident Response Plan (Tool #22).

Privacy and Security Breach Investigation Report

INSERT YOUR LOGO HERE

Date Reported: _____ (YYYY/MM/DD)

Incident Number (optional): _____

To be completed by the individual reporting the incident			
A. Reporting Person's Information			
Name:		Phone #:	
Email:		Position:	
Any others who may have witnessed the incident or may have additional information:			

B. Incident Information			
Date Incident Occurred:		Date Incident Detected:	
	(YYYY/MM/DD)		(YYYY/MM/DD)
Incident Location:			
General Description of the Incident:			
Media / Device Type (if applicable):			
If yes, was the Media / Device Encrypted?	☐ Yes ☐ No ☐ Unknown		
If yes, what information may have been on the Media / Device (list all that you think of/know of):			

To be completed by the Investigator			
C. Incident Details			
Was personal health information (PHI) involved that could identify a client?	☐ Yes ☐ No		
☐ Name ☐ Family Information ☐ Contact Information ☐ Other (specify)	☐ Social Insurance Number ☐ Health Card ☐ First Nation Information	☐ Financial Information ☐ Health/Medical Information	
Number of individuals potentially affected:		Date of notification (if required):	
			(YYYY/MM/DD)
Was information identifying a First Nation involved (eg. Aggregate reports):	☐ Yes ☐ No		
Is a notification required through any other policy? (eg. First Nations Management)	☐ Yes ☐ No		
Is a consultation required with other health facility resources to provide advice?	☐ Legal ☐ IT ☐ Other		
Is a Privacy Disclosure Notification Required? (Tool #24)	☐ Yes ☐ No		
If no, provide explanation:			
Result of investigation	☐ Incident (only) ☐ Breach		

D. Containment and Preventive Actions			
Containment			
Please describe containment activities. (Such as retrieval of device or files, change of passwords and locks, etc.)			
Actions (check all that apply)	Description		
☐ Notification to Client (Tool #24)		Date	
☐ Notification to Privacy Commissioner		Date	
☐ Notification to Other		Date	
☐ Notification to Other		Date	
Preventive Actions			
Action (check all that apply)	Description		
☐ Policy/Procedure revisions/updates			
☐ Training			
☐ Disciplinary			
☐ Technology/Physical Prevention			
☐ Police Support			
☐ Other			
E. Approvals			
Health Facility Management:		Date	
			(YYYY/MM/DD)
Privacy Contact:		Date	
			(YYYY/MM/DD)

Tool #24
Notice of Breach – Letter to Clients

Instructions

If your health facility does not have an existing letter prepared for privacy breaches, you can use this template to contact individuals whose information has been (or is at risk of being) improperly accessed or disclosed.

INSERT YOUR LOGO HERE

<Date>

<Name of Individual>

<Address>

<City>, <Province>

<Postal Code>

Re: <Insert reason for letter>

Dear <Name of Individual>,

On behalf of <First Nation Health Facility>, I regret to inform you that we believe your personal health information has been <choose one or more: lost/stolen/inappropriately accessed>. We are in the process of investigating this incident and are taking the following steps:

[List the steps that you are doing to correct use or sharing of the person's personal health information]

- Step 1
- Step 2
- Step 3
- Etc.

<First Nation Health Facility> takes issues related to individual privacy very seriously and we are committed to keeping our clients' personal health information safe and confidential.

If you have any questions or concerns, please contact <Privacy Contact> at <contact information>.

You can also contact the Information and Privacy Commissioner's Office at:

Information and Privacy Commissioner/Ontario,

2 Bloor Street East, Suite 1400, Toronto, Ontario M4W 1A8

Tel: (416) 326-3333 Toll-free: 1-800-387-0073

Yours truly,

<name of Privacy Officer>

<name of agency>

<address>

<other contact information>

cc: <include applicable individuals>

Appendix A
Glossary

There are terms used throughout this document that have specific meanings:

Term	Definition
Acceptable Use	A set of rules describing the approved types of behaviour and use of the electronic network and/or information technology (IT) systems of a Health Organization.
Access Control	A term used in computer security that involves controlling who can see or use particular information or use systems. Examples of access controls include authentication (making sure the person is who they say they are), authorization (making sure they have approval to access Personal Health Information) and audit (tracking activity). Access control includes measures such as physical devices, including digital signatures, encryption, and training.
Agent	According to the Personal Health Information Protection Act (PHIPA), an agent is a person with the authority to act on behalf of the Health Information Custodian with respect to Personal Health Information. The agent acts for the purposes of the Health Information Custodian, and not their own. First Nation Health Organizations are Health Information Custodians and the staff, contractors, students and volunteers are "agents".
Aggregate information	Information in summary form about a group of individuals in which individual identifying information has been removed (such as a immunization coverage report). Aggregate information is not regulated by the Personal Health Information Protection Act (PHIPA).
Assets	Any information, device, or other component that supports information-related activities including hardware, software, laptops, or other mobile devices and confidential information such as Personal Health Information.
Audit	A formal review of user activities in a computer system. For example, audit reports could be created that identify the: clients whose records were accessed by a particular user; users who accessed a particular client's records.
Authentication	The process of confirming a user's identity, typically through a password or certificate process.
Authorization, Authorized (IT)	Authorization refers to the process of deciding what information and systems a user is allowed to access based on their identity. A user

Term	Definition
	becomes authorized to access a system based on their role and need to access information.
Authorization, Authorized (Management)	Authorization refers to providing approval for staff, contractors, students or volunteers.
Backup, Backing Up	The process of making copies of information that may be used to restore the original after any type of loss.
Breach	A PHIPA(Personal Health Information Protection Act) “breach” happens if Personal Health Information is used or disclosed in a way that does not follow the privacy duties of a Health Information Custodian under PHIPA . A Policy breach happens when any of the health facilities’ policies are not followed.
Business Continuity Management Plan (BCP)	This refers to planning for continuing an organization’s operations if serious events happen - such as a fire, flood, power failure, vandalism, computer failure, pandemic or other disruption. The BCP may already be included in an Emergency Preparedness Plan (EPP).
Capacity to Consent	The Ontario Health Care Consent Act says that a person has capacity if they are “able to understand the information that is relevant to making a decision about the treatment, admission or personal assistance service” and can understand the potential consequences of making, or not making, a decision (Sec. 4)
Client	An individual who receives service from a Health Organization and has a record in any paper or electronic health information management system.
Collect, Collection	To gather, assemble or receive Personal Health Information by any means from any source.
Confidentiality	Confidentiality is the concept of not sharing client information or other sensitive information that has been collected by a health care provider.
Consent	Consent is the permission that a person gives for the collection, use or sharing of his/her Personal Health Information. See also: Express Consent, Implied Consent, and Informed Consent.
Containment	Containment refers to the activities required to minimize the impact of a breach.
Custody or Control (of Information)	Custody or control refers to a Health Information Custodian’s responsibilities in relation to the Personal Health Information they collect, whether it is in their health facility or housed elsewhere (e.g. remote server, USBs, Panorama).

Term	Definition
Demographic Information	Information that describes a person or a population that can be used to support administrative decisions or for summary reports. Typical demographic details include age, gender and location.
Digital Signatures	A digital signature is a method to ensure that an electronic message or document is trustworthy. A digital signature on a transmitted file lets the receiver know that the message was created by a known sender, and that it was not altered after being sent.
Disclose, Disclosure	In relation to Personal Health Information in the custody or under the control of a Health Information Custodian or a person, disclosure means to share, release, or make the information available to another Health Information Custodian or to a person outside the health facility.
Emergency Preparedness Plan (EPP).	See Business Continuity Management Plan.
Encryption	Encryption is the process of changing information so it is unreadable to anyone except those with a special “key”.
Express Consent	Express Consent is when an individual is asked for their consent before any collection, use or disclosure of Personal Health Information. Express Consent can be verbal or in writing.
Hacker, Hack	A hacker is someone who breaks into a secure system for fun or profit, and possibly steals information or damages information.
Health Information Custodian	A Health Information Custodian (HIC) is a person or organization that has custody or control of Personal Health Information as a result of their duties.
Identifying Information	Information, either alone or together with other information, that tells who an individual is. This can include name, birth date, address, Band Number, etc.
Implied Consent	Implied Consent is when Health Information Custodians are entitled to assume that an individual has given consent to the collection, use or disclosure of his/her Personal Health Information for the delivery of health care service or treatment.
Incident	An incident is an unwanted or unplanned event that creates the potential for a breach that may compromise the confidentiality, integrity, and/or availability of sensitive information.
Information Practices	The set of practices used by the Health Information Custodian relating to Personal Health Information, including

Term	Definition
	when, how, and the purposes for which the Health Information Custodian collects, uses, changes, discloses, stores, or disposes of Personal Health Information; and the administrative, technical, and physical protection and practices that the Health Information Custodian performs.
Information and Privacy Commissioner (IPC)	The IPC is an Ontario official who is responsible for oversight of the Personal Health Information Protection Act (PHIPA).
Information Retention	The act of storing information for a specific length of time before it is erased, deleted or destroyed.
Information Technology, IT	The technology involving the development, maintenance, and use of computer systems, software, and networks for the processing and distribution of data.[5]
Information Security	The protection of information to prevent loss, access or misuse. It includes the ongoing process of assessing threats and risks to information.
Informed Consent	Informed Consent means that the client is "knowledgeable" about the decision to which they are consenting. This principle applies to all forms of consent including consent for treatment, and collection, use, or disclosure of Personal Health Information.
Initial Subscribers	The First Nations that will be the first in Ontario to use Panorama.
Log Files	A log file is a record of user activity in a computer system.
Malicious Software / Malware	This is software used by hackers to disturb computer systems, gather sensitive information, or gain illegal access to computer systems. "Malware" is a short name for Malicious Software used by computer professionals to include computer viruses, worms, Trojan horses, spyware, adware, and other harmful programs.
Mobile Device	A mobile device (also known as a handheld device, handheld computer or simply as a handheld) is a small, hand-held computing device, typically having a display screen with touch control and/or a miniature keyboard and weighing less than 2 pounds. Examples include smart phones and iPads.
Panorama	A web-based information system that will assist First Nations and public health professionals to manage public health programs and communicable disease cases and outbreaks. Panorama includes seven

[5] www.Merriam-Webster.com

Term	Definition
	units that can be implemented separately or together: Investigations, Outbreak Management, Immunization, Inventory, Family Health, Work Management and Notifications.
Patch	Software designed to fix problems with, or update a computer program. This includes fixing security gaps and improving system performance.
Permission	Software-based authorization to perform specific actions in a computer system.
Personal Health Information (PHI)	Personal Health Information is identifying information about an individual in verbal or written form, if the information: relates to the physical or mental health of the individual, including information a family health history relates to providing health care to the individual, including identifying a health care provider for the individual is a plan of service for the individual as defined by the Long-Term Care Act, 1994 relates to payments or eligibility for health care relates to the donation, testing, or examination of any body part or bodily substance is the individual's health number identifies an individual's substitute decision-maker.
Personal Health Information Protection Act (PHIPA)	The Ontario law that sets out the duties of Health Information Custodians to protect the privacy of Personal Health Information and to ensure the informed consent of clients for the collection, use, and disclosure of their Personal Health Information. The law applies to the Health Information Custodians identified in the Act, including First Nation Health Organizations.
Privacy (of Personal Health Information)	The right of individuals to decide what information is collected about them, how it is used, and to whom it is disclosed.
Privacy Breach	See Breach
Privacy Contact or Privacy Officer	The contact person formally assigned by the Health Organization to answer questions from clients and the public about the Health Organization's privacy and information practices. This is a requirement in the Personal Health Information Protection Act (PHIPA).
Privacy Impact Assessment	A detailed, formal review and evaluation of the information privacy issues and risks associated with a new system or process. A PIA is also best practice when there are major changes to important systems or processes.

Term	Definition
Recipient	Third parties who hold Personal Health Information outside the health sector and are not covered under the Personal Health Information Protection Act (PHIPA) (such as insurance companies, employers, school boards and others).
Record	An account of information kept in any form or in any medium, whether written, printed, photographic, electronic, or other form.
Registration (User)	Registration is the process of assigning system access credentials to an individual so they can use the Health Organization network and information management system. De-registration is the process of removing system access credentials from an individual.
Restore	Restoring means replacing system files, installed programs, etc., to a previous state in the event of a loss or system failure.
Retention	The storage of Personal Health Information for a period of time as required by professional health care bodies, organization policies, or by data sharing agreements.
Role / Role-Based Access	Role based access means that permission to access Personal Health Information or information systems will be granted depending on the user's role in a Health Organization.
Safeguard	A device or measure designed to protect an asset and is part of a Health Organization's system security. Safeguards include user identification and password access, authentication, access rights and authority levels.
Security (of Personal Health Information)	The controls or processes that are put in place to ensure the confidentiality of information, and protect privacy of Personal Health Information and other information. Examples include passwords to access computers, proper storage of clinical files, locked doors, and policies and procedures.
Threat	A possible danger that might find a security gap and cause possible harm. A threat can be either: "intentional" – such as an individual system hacker or a criminal organization. It can also include an approved user deliberately accessing information improperly "accidental" – such as the possibility of a computer malfunctioning, or the possibility of natural disaster as an earthquake, a fire, a tornado or other event.
Timeout	A commonly used system security process that disconnects a system user if they have not been using the system for a period of time.

Term	Definition
Use	In the Personal Health Information Protection Act (PHIPA), “use” means to handle or deal with the Personal Health Information in the custody or under the control of a Health Information Custodian, but does not include the disclosure of information.
Vulnerability	A weakness that leaves a computer system open to attack, reducing confidence that system's information is secure.

Appendix B

Health Information Custodian Responsibilities According to PHIPA

This Appendix identifies the responsibilities of a Health Information Custodian (HIC) for Privacy and Security practices as they relate to PHI in accordance with PHIPA.

In general terms, HICs must apply and follow certain PHI practices including:

- Identifying a Privacy Contact responsible for following PHIPA rules, and responding to questions, access requests, correction requests, or complaints
- Making a Privacy Notice available that describes PHI practices
- Developing policies and procedures to support the collection, use, and disclosure of PHI including privacy or security breaches, record keeping and destruction
- Limiting the collection, use, and disclosure of PHI to only what is necessary to meet the purposes identified in the Privacy Notice
- Following steps to ensure PHI is accurate
- Maintaining physical, technical, and administrative controls to keep PHI safe and support secure disposal
- Developing a process to manage user accounts so only authorized users providing health care services or other approved activities have access to PHI6
- Providing access to or correction of a client's PHI upon written client request, subject to some exceptions (PHIPA Sections 52 and 55)
- Notifying affected individuals of privacy breaches.

[6] O.Reg 329/04 sec. 6 makes a requirement for HICs using a health information network provider (HINP) to support their electronic systems. PHIPA sec. 12(1) states that HICs "shall take steps that are reasonable in the circumstances to ensure that PHI in the custodian's custody or control is protected against theft, loss and unauthorized use or disclosure and to ensure that the records containing the information are protected against unauthorized copying, modification or disposal."

Appendix C

Additional Resources

The following are additional resources on privacy that you may find helpful for further information.

1. A Guide to the Personal Health Information Protection Act

Information and Privacy Commissioner of Ontario, (2004).

This guide was created to give HICs a basic understanding of how the Personal Health Information Protection Act (the Act) applies in the course of day-to-day activities. It has been designed to help HICs understand their rights and obligations under the legislation. The guide provides information about how the legislation will apply in some common scenarios and provides answers to the most frequently asked questions of HICs.

Web: http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=400

Phone: 1-800-387-0073

2. Circle of Care: Sharing Personal Health Information for Health-Care Purposes

Information and Privacy Commissioner of Ontario, (2009).

This brochure was developed to clarify the circumstances in which a HIC may assume implied consent, and provide options available to the HIC when consent cannot be assumed to be implied.

Web: http://www.ipc.on.ca/english/Resources/Best-Practices-and-Professional-Guidelines/Best-Practices-and-Professional-Guidelines-Summary/?id=885

Phone: 1-800-387-0073

3. Fact Sheet #01 – Safeguarding Personal Health Information

Information and Privacy Commissioner of Ontario (2005).

The purpose of this fact sheet is to highlight some important safeguards for protecting PHI. The Information and Privacy Commissioner (IPC) web site under the "Resources" section includes a number of other Fact Sheets on various privacy-related topics.

Web: http://www.ipc.on.ca/English/Resources/Educational-Material/Educational-Material-Summary/?id=181

Phone: 1-800-387-0073

4. Practice Standard: Confidentiality and Privacy – Personal Health Information

College of Nurses of Ontario, (2009).

This document provides an overview of Ontario's current legislation including the Personal Health Information Protection Act, and clarifies nursing standards for confidentiality and privacy of PHI. The document includes Standard Statements and the best practice indicators that the standards are being achieved.

Web: http://www.cno.org/learn-about-standards-guidelines/publications-list/standards-and-guidelines/

Phone: 1-800-387-5526

5. Practice Standard: Documentation

College of Nurses of Ontario, (2009).

This practice standard explains the legal requirements for nursing documentation. The content is divided into three standard "statements" that describe broad practice principles. Each statement is then followed by a set of indicators that outline a nurse's accountability when documenting and assist with applying the standard statements in various situations.

Web: http://www.cno.org/learn-about-standards-guidelines/publications-list/standards-and-guidelines/

Phone: 1-800-387-5526

6. Practice Guideline: Consent

College of Nurses of Ontario, (2009).

This practice guideline provides an overview of the major features of the Health Care Consent Act and the Substitute Decisions Act, relevant definitions, the steps nurses need to take to obtain consent, and the guidelines for nurses advocating for clients found incapable of making certain decisions. It does not address consent under the Mental Health Act.

Web: http://www.cno.org/learn-about-standards-guidelines/publications-list/standards-and-guidelines/

Phone: 1-800-387-5526

7. Personal Health Information Protection Act, 2004

Province of Ontario, (2004).

Full text of the statute.

Web: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_04p03_e.htm

8. Ontario Regular 329/04: Personal Health Information Act, 2004

Province of Ontario, (2004).

Full text of the PHIPA Regulation.

Web: http://www.e-laws.gov.on.ca/html/regs/english/elaws_regs_040329_e.htm

9. Substitute Decisions Act, 1992

Province of Ontario, (1992).

Full text of the statute.

Web: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_92s30_e.htm

10. An overview of Techniques for De-Identifying Personal Health Information

El Emam, K., & Fineberg, A., (2009, August).

This report describes methods to de-identify PHI.

Web: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1456490

11. Dispelling the Myths Surrounding De-identification: Anonymization Remains a Strong Tool for Protecting Privacy

Covoukian, A. & El Emam, K., (2011, June).

This paper explains the importance of de-identifying personal information before collection, use, or disclosure.

Web: http://www.ipc.on.ca/English/Resources/Discussion-Papers/Discussion-Papers-Summary/?id=1084

12. Health Care Consent Act, 2004

Province of Ontario, (2004)

This law addresses client rights to consent to treatment by a registered health care provider. Particular sections of interest may include:

- Elements of consent (sec. 11)
- Capacity (sec. 15-19)
- Substitute decision-making (sec. 20-24)
- Emergency treatment (sec. 25-28)
- Consent and Capacity Board (Part V)

Web: http://www.e-laws.gov.on.ca/html/statutes/english/elaws_statutes_96h02_e.htm

13. Consent and Capacity Board

Queen's Printer for Ontario, (2005).

The Consent and Capacity Board is an independent body created by the government of Ontario under the Health Care Consent Act. It conducts hearings under the Mental Health Act, the Health Care Consent Act, the Personal Health Information Protection Act, the Substitute Decisions Act and the Mandatory Blood Testing Act. Board members are psychiatrists, lawyers and members of the general public appointed by the Lieutenant Governor in Council.

Web: http://www.ccboard.on.ca/scripts/english/index.asp

14. CPSO Medical Records Policy: Retention, Access and Transfer of Medical Records

College of Physicians and Surgeons of Ontario

This document (sec. 4) details the medical records retention policy recommendations for physicians practicing in Ontario. The CPSO recommendations are based on the Medicine Act but extends the Act's minimum retention requirement from 10 to 15 years.

Web: http://www.cpso.on.ca/policies/policies/default.aspx?ID=1686

15. Ownership Control Access and Possession (OCAP)

Assembly of First Nations, June 2007

This document provides an overview of the principles of Ownership, Control, Access and Possession as they refer to First Nations cultural knowledge, data and information.

http://64.26.129.156/misc/ocap.pdf